

McAfee Policy Auditor 5.0 Product Guide

COPYRIGHT

Copyright © 2008 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEES SECURITYALLIANCE EXCHANGE), MCAFEES, MCAFEES.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEES OR THE PLACE OF PURCHASE FOR A FULL REFUND.

License Attributions

Refer to the product Release Notes.

Contents

Introducing McAfee Policy Auditor 5.0.....	8
Policy Auditor components and what they do.....	9
Policy Auditor.....	9
Policy Auditor Agent Plug-in.....	9
Benchmark Editor.....	9
Using this guide.....	10
Where to find McAfee product information.....	11
Configuring Policy Auditor.....	12
How benchmarks work.....	12
Server setting categories.....	13
Audit score category.....	13
Default scoring model.....	13
Audit score.....	13
Audit label.....	14
Data retention.....	14
Stop data maintenance.....	14
How permission sets work.....	14
Built-in permission sets.....	15
Policy Auditor Agent Plug-in.....	16
Editing server settings.....	16
Managing Policy Auditor permission sets.....	16
Creating a permission set.....	16
Duplicating a permission set.....	17
Editing a permission set.....	17
Deleting a permission set.....	18
Complying with SCAP.....	19
Statement of FDCC Compliance.....	19
Statement of SCAP Implementation.....	19
Statement of CVE Implementation.....	20
Statement of CCE Implementation.....	20
Statement of CPE Implementation.....	20

Statement of CVSS Implementation.	20
Statement of XCCDF Implementation.	21
Statement of OVAL Implementation.	21
Managing the Policy Auditor Agent Plug-in.	22
The Policy Auditor Agent Plug-in and how it works.	22
Supported platforms.	23
Managing content.	23
Working with the McAfee Policy Auditor Agent Plug-in.	24
Sending manual wake-up calls to a group.	24
Deploying the Policy Auditor Agent Plug-in.	25
Determining whether the Agent Plug-in is being deployed.	26
Verifying that the Agent Plug-in has been deployed.	26
Verifying that the agent and server are communicating.	26
Uninstalling the Policy Auditor Agent Plug-in.	27
Determining whether the Agent Plug-in is being removed.	28
Verifying that the Agent Plug-in has been uninstalled.	28
Creating and Managing Audits.	30
Audits and how they work.	31
Considerations for including systems in an audit.	32
Benchmark profiles and their impact on managed systems.	34
Benchmark labels and how they can aid in creating audits.	34
Audit frequency.	34
Audit whiteout and blackout periods.	34
How viewing audit results works.	35
Audit exports.	36
Setting whiteout and blackout periods.	36
Exporting audits to XCCDF.	37
Exporting audits to OVAL.	37
Creating a new audit.	37
Selecting benchmarks.	38
Editing existing audits.	40
Deleting Audits.	42
Scoring Audits.	43
Score computation algorithms.	43
Default scoring model.	43
Flat scoring model.	43

Flat unweighted scoring model.....	44
Absolute scoring model.....	44
Changing the scoring model.....	44
Creating and Managing Waivers.....	45
How waivers work.....	46
Waivers catalog.....	46
Types of waivers.....	47
Exception waivers.....	47
Exemption waivers.....	47
Suppression waivers.....	48
Waiver status.....	48
Waiver benchmark and rule management.....	48
How start dates and expires dates work.....	49
Filtering waivers.....	49
Filtering waivers by status.....	50
Filtering waivers as of a specified date.....	50
Filtering waivers by group.....	51
Requesting waivers.....	51
Granting waivers.....	52
Expiring waivers.....	53
Deleting waivers.....	53
Managing Issues and Tickets.....	54
Issues and how they work.....	54
How issues are created.....	54
How issues are managed.....	55
Tickets and how they work.....	55
How tickets are created.....	55
How ticketed issues are assigned.....	55
How tickets and ticketed issues are closed.....	55
Why ticketed issues should not be edited manually.....	56
How comments are handled.....	56
How tickets are reopened.....	56
How ticketed issues are synchronized.....	56
Integrations with ticketing servers.....	57
Considerations when deleting a registered ticketing server.....	57
Required fields for mapping.....	57
Sample mappings.....	58

Working with issues.	60
Creating issues.	60
Creating issues automatically with responses.	61
Assigning issues.	62
Viewing the details of issues.	62
Adding comments to issues.	62
Editing issues.	63
Deleting issues.	63
Purging closed issues.	63
Purging closed issues on a schedule.	63
Working with ticketing servers.	64
Installing extensions for ticketing servers.	64
Registering and mapping a ticketing server.	67
Upgrading a registered ticketing server.	70
Working with tickets.	71
Adding tickets to issues.	71
Synchronizing ticketed issues.	72
Synchronizing ticketed issues on a schedule.	72
Querying the Database.	73
Queries.	73
Public and personal queries.	74
Query permissions.	74
Query Builder.	75
Multi-server roll-up querying.	76
Preparing for roll-up querying.	76
Registering ePO servers.	77
Creating a Data Roll Up server task.	77
Working with queries.	78
Creating custom queries.	78
Running an existing query.	79
Running a query on a schedule.	79
Making personal queries public.	81
Duplicating queries.	81
Sharing a query between ePO servers.	81
Exporting query results to other formats.	82
Default queries and what they display.	83
PA: Benchmark Checks.	83

PA: Benchmark Rules.	83
PA: Checks Across Benchmarks.	83
PA: Check Catalog List.	83
PA: Check Catalog Usage List.	84
PA: Systems by Audit.	84
PA: Trend of Benchmarks Reported as Failed.	84
PA: Trend of Checks Reporting as False.	84
PA: Trend of Rules Reporting as Failed.	85
Assessing Your Environment With Dashboards.	86
Dashboards and how they work.	86
Queries as dashboard monitors.	86
Default dashboard monitors.	86
Setting up dashboard access and behavior.	87
Giving users permissions to dashboards.	87
Configuring the refresh frequency of dashboards.	87
Working with Dashboards.	88
Creating dashboards.	88
Making a dashboard active.	88
Selecting all active dashboards.	89
Making a dashboard public.	89

Introducing McAfee Policy Auditor 5.0

McAfee Policy Auditor evaluates the status of managed systems relative to audits that contain benchmarks. Benchmarks contain rules that describe the desired state of a managed system. Benchmarks are received through or imported into McAfee Benchmark Editor and, once activated, can be used by Policy Auditor. Benchmarks are written in the open-source XML standard formats Extensible Configuration Checklist Description Format (XCCDF) and the Open Vulnerability Assessment Language (OVAL). XCCDF describes what to check while OVAL specifies how to perform the check.

Policy Audit

☐ Benchmarks	(XCCDF)
☐ Profiles	(XCCDF) - Optional
☐ Groups	(XCCDF)
☐ Rules	(XCCDF / OVAL)
☐ Checks	(OVAL)
☒ Values	(XCCDF)
☒ Systems / Groups / Devices	(ePO System Tree)
☒ Audit Frequency	(PA 5)
☒ Waivers	(PA 5) - Optional

Figure 1: Policy Audit Tree

You can create audits, adjust settings to determine when and how often they are run, and use the results of audits to report on the historical status of your managed systems. The customizable reporting system provides you quick access to information such as policy audit status, exposure to threats, and overall risk. You can also view a summary of the status of your managed systems on the Dashboards page.

Policy Auditor allows you to conduct audits on various releases of the following operating systems:

- Microsoft Windows
- Macintosh OS X
- HP-UX
- Solaris
- Red Hat Linux

Policy Auditor can be integrated with third-party trouble ticketing systems to generate issues or tickets whenever an audit discovers a security threat or misconfiguration. Policy Auditor marks issues as resolved upon ticket closure.

Contents

- ▶ [Policy Auditor components and what they do](#)
- ▶ [Where to find McAfee product information](#)

Policy Auditor components and what they do

McAfee Policy Auditor 5.0 consists of three components that enable you to analyze managed systems for compliance with authoritative, open source comppliance standards.

- **Policy Auditor** — manages all aspects of analyzing managed systems for compliance.
- **Policy Auditor Agent Plug-in** — The agent plug-in extends the McAfee agent as a vehicle of information between the server and each managed system. The agent receives audits from Policy Auditor, ensures that audits are run as scheduled, and returns the results to Policy Auditor.
- **Benchmark Editor** — This tool allows you to manage and create benchmarks. Benchmarks contain information about the desired state of the managed system.

Policy Auditor

McAfee Policy Auditor analyzes managed systems to determine whether they comply with user-defined audits. Audits are composed of benchmarks that are generally supplied by McAfee, but may be imported from third-party sources or created by yourself using Benchmark Editor. You must activate received or imported benchmarks in Benchmark Editor before you can use them in audits. Benchmarks contain rules that describe the desired state of a managed system.

Policy Auditor Agent Plug-in

The Policy Auditor Agent is a plug-in to the McAfee Agent. It extends the features of the McAfee Agent to support Policy Auditor. When audits are deployed to the McAfee Agent, the Policy Auditor Agent Plug-in decides when the audits can be run. The Agent Plug-in conducts the audits at the appropriate time and returns the results to the ePO server. The Policy Auditor Agent Plug-in can even conduct audits when the managed system is off the network and then return results to the ePO server once the system is re-attached to the network.

Benchmark Editor

Benchmark Editor allows you to create and edit benchmarks. Benchmarks contain rules that define the state of a managed system. The ePO server automatically provides benchmarks to the Benchmark Editor. Normally, you activate the benchmarks when they are received so that they can be used in audits.

Tailoring is a way to customize certain aspects of benchmarks. You can tailor McAfee-provided benchmarks but you cannot edit them. You may also create your own benchmarks or import them from third-party sources. Benchmarks that are not supplied by McAfee may be tailored or edited.

Using this guide

This guide provides basic information on configuring Policy Auditor. For information on configuring the ePO server, refer to the *McAfee ePolicy Orchestrator 4.0.2 Product Guide*.

This guide provides information on configuring and using your product. For system requirements and installation instructions, see the *Installation Guide*.

This material is organized in the order that McAfee recommends to set up Policy Auditor in a production environment for the first time, and is also accessible to anyone seeking specific topics.

Setting up Policy Auditor for the first time?

This guide serves as a tool to help administrators set up Policy Auditor for the first time, and as a reference tool for more experienced users. Depending on your environment, you may perform some of these tasks in a slightly different order.

This guide assumes that you have already set up the ePO server; if you have not done so, set up the ePO server according to the *McAfee ePolicy Orchestrator 4.0.2 Product Guide*. You should also become familiar with activating benchmarks for use in audits. This information may be found in the *McAfee Benchmark Editor 5.0 Product Guide*.

McAfee recommends setting up Policy Auditor in this order:

- 1 Configure Policy Auditor** — Set up user accounts and permissions, configure settings, and get familiar with the user interface.
- 2 Deploy the McAfee Agent Plug-in** — Each system you manage must have the McAfee Agent Plug-in installed. This section provides detailed information on distributing and maintaining the McAfee Agent Plug-in in your environment.
- 3 Create Audits** — Create audits using activated audits from Benchmark Editor. Set up the audit frequency and define audit whiteout and blackout periods for each audit.
- 4 Create Waivers** — You may have some systems that you do not want to audit or show their scores. Create waivers for these systems.
- 5 Integrate Policy Auditor with your Ticketing System** — Policy Auditor is able to integrate with a number of commonly-used ticketing systems and to create issues and responses to issues.**Configure Dashboards** — Policy Auditor has a built-in dashboard that is suitable for most needs. However, the application gives you the ability to create new dashboards to meet your organization's requirements.
- 6 Configure Dashboards** — Policy Auditor has a built-in dashboard that is suitable for most needs. However, the application gives you the ability to create new dashboards to meet your organization's requirements.
- 7 Customize Reporting** — Policy Auditor has a rich system to build queries and create reports. The application comes with a number of built-in reports that are sufficient for most situations, but you may want to create additional reports to fit your needs.
- 8 Configure Dashboards** — Policy Auditor has a built-in dashboard that is suitable for most needs. However, the application gives you the ability to create new dashboards to meet your organization's requirements.

Audience

This information is intended for network administrators who are responsible for their company's security program.

This guide assumes that the customer has already installed ePolicy Orchestrator (ePO) server.

Where to find McAfee product information

The McAfee documentation is designed to provide you with the information you need during each phase of product implementation, from evaluating a new product to maintaining existing ones. Depending on the product, additional documents might be available. After a product is released additional information regarding the product is entered into the online Knowledgebase available on McAfee ServicePortal.

Evaluation Phase	Installation Phase	Setup Phase	Maintenance Phase
How can my company benefit from this product? <i>Evaluation Tutorial</i>	Before, during, and after installation. <i>Release Notes</i>	Getting up-and-running with the product. <i>Product Guide and Online Help</i>	Maintaining the software. <i>Online Help</i>
- Preparing for, installing and deploying software in a test environment. - Detailed instructions for common tasks.	- Known issues in the current release. - Issues resolved since the last release. - Last-minute changes to the product or its documentation. <i>Installation Guide</i> - Preparing for, installing and deploying software in a production environment.	- Setting up and customizing the software for your environment. <i>Online Help</i> - Managing and deploying products through ePolicy Orchestrator. - Detailed information about options in the product.	- Maintaining the software. - Reference information. - All information found in the product guide. <i>Quick Reference Card</i> - Detailed instructions for common and infrequent important tasks. <i>Knowledgebase</i> - Release notes and documentation. - Supplemental product information. - Workarounds to known issues.

Finding release notes and documentation for Policy Auditor

- 1 Go to the [McAfee ServicePortal](#) and select **Product Documentation** under **Useful links**.
- 2 Select **Policy Auditor | 5.0** and select the required document from the list of documents.

Configuring Policy Auditor

Policy Auditor is configured from the ePO Server. The ePO Server is the center of your managed environment and provides a single location from which you can administer security settings throughout your network.

Are you configuring Policy Auditor for the first time?

When configuring Policy Auditor for the first time:

- Understand what server settings are and how they work
- Understand what permission sets are and how they work
- Understand the built-in permissions sets for Policy Auditor and Benchmark Editor. The built-in permission sets are suitable for the needs of most organizations.
- Ensure that users are assigned to permissions sets that fit their roles in your organization.

Contents

- ▶ [How benchmarks work](#)
- ▶ [Server setting categories](#)
- ▶ [How permission sets work](#)
- ▶ [Built-in permission sets](#)
- ▶ [Policy Auditor Agent Plug-in](#)
- ▶ [Editing server settings](#)
- ▶ [Managing Policy Auditor permission sets](#)

How benchmarks work

Benchmarks are written in the Extensible Configuration Checklist Description Format (XCCDF) language, which is based on the Extensible Markup Language (XML). The basic unit of the benchmark is a rule. Rules contain checks, which are usually in the form of an OVAL definition. Checks are not limited to OVAL definitions though, and may be in other formats such as a file or file reference.

The Open Vulnerability and Assessment Language (OVAL) is an international standard that promotes openly-available security content. It is the common language for security experts to check for the presence of vulnerabilities and configuration issues on managed systems. OVAL definitions provide a structured model for network and system administrators to detect vulnerabilities and configuration issues on managed systems.

McAfee uses the term check for objects that may be OVAL definitions or other formats supported by XCCDF.

Benchmarks contain a structured collection of security configurations for managed systems. Benchmarks determine whether a system complies to the rules that it contains. Not only do

benchmarks determine compliance with its rules, but they also return results that can be converted to a human-readable format.

Server setting categories

You should configure Policy Auditor's server settings before you begin using the product. McAfee supplies default settings, but you might want to use different server settings to fit your organizational needs.

These server setting category sections describe each setting, thus helping you to make informed decisions as to whether you should change the default settings.

Audit score category

Policy Auditor allows you to set the names used to describe the four audit score categories. McAfee recommends that you keep the default settings but you may change them to fit your organizational needs or existing security policies.

Audit Score Category	Description
Audit score - Category High	High
Audit score - Category Low	Low
Audit score - Category Medium	Medium
Audit score - Category Unknown	Unknown

Default scoring model

Policy Auditor supports the four standard XCCDF scoring models. These scoring models are described in more detail in the *Scoring Audits* section. Policy Auditor uses the flat unweighted scoring model normalized to a value of 100 as its default scoring model.

Audit score

Policy Auditor allows you to change the default score in order to help you determine a score that constitutes passing an audit or failing an audit. A score equal to or less than the Maximum Low Score is considered be below the desired level that you want a system to achieve.

Audit Score	Description
Maximum Low Score	Any audit score below this setting will have a category of Low if you use the default settings.
Minimum High Score	Any audit score above this setting will have a category of High if you use the default settings
Audit Score - Fail	Any audit score below this setting means that the audit has failed.

Audit label

Policy Auditor allows you to set the names used to describe whether an audit has a status of pass, fail, or unknown. McAfee recommends that you keep the default settings but you may change them to fit your organizational needs or existing security policies.

Audit Score Category	Default setting
Audit label - Fail	Fail
Audit label - Pass	Pass
Audit label - Unknown	Unknown

Data retention

Altering the Data Retention allows you to set how long Policy Auditor retains its audit data. The **Data Retention Unit Type** setting offers you 4 time periods to choose from:

- Days
- Weeks
- Months
- Years

The **Data Retention Units** setting allows you to specify the units of time in conjunction with the **Data Retention Unit Type** setting.

- **Example 1** — You set the **Data Retention Unit Type** to weeks and the **Data Retention Units** to 12. This means that your audit data will be retained for 12 weeks before deletion.
- **Example 2** — You set the **Data Retention Unit Type** to years and the **Data Retention Units** to 2. This means that your audit data will be retained for 2 years before deletion.

Note that the longer you retain your data, the more disk space you will need.

Stop data maintenance

Processing numerous audits from a large number of machines can be CPU and memory-intensive and will slow down the ePO Server user interface. Setting **Stop data maintenance** will tell Policy Auditor how long it is able to perform data maintenance before temporarily stopping the processing. When data maintenance restarts, it will begin where it left off.

How permission sets work

A permission set is a group of permissions, divided in sections, that can be granted to any user by assigning it to a user's account. One or more permission sets can be assigned to any user that is not a global administrator. Global administrators have all permissions to all products and features.

Permission sets grant permissions only — no permission set ever removes a permission.

When are permission sets assigned?

Global administrators can assign existing permission sets when creating or editing user accounts and when creating or editing permission sets.

What happens when I install new products?

When a new extension is installed it might add one or more sections to the permission sets. For example, when you install a Policy Auditor extension, a Policy Auditor section is added to each permission set. Initially, the newly added section is listed in each permission set with no permissions configured. A global administrator can then grant permissions in the new section.

Built-in permission sets

Policy Auditor installs the following built-in permission sets:

Permission Set	Permissions
PA Admin	- Benchmark Editor: Create, delete and import checks - Benchmark Editor: Create, delete, modify, import and unlock benchmarks - Benchmark Editor: Activate benchmarks - Benchmark Editor: Create, delete and apply labels - Benchmark Editor: Edit benchmark tailoring - Issue Management: Create, edit, view and purge assigned issues - Policy Auditor: Grant and modify Waivers - Policy Auditor: Add, remove, and change Audits and Assignments - Policy Auditor Agent: View and change settings
PA Agent Admin	Policy Auditor Agent: View and change settings
PA Audit Admin	- Benchmark Editor: View and export benchmarks - Benchmark Editor: View and export checks - Policy Auditor: Add, remove, and change Audits and Assignments - Policy Auditor: View Waivers
PA Benchmark Activator	- Benchmark Editor: View and export benchmarks - Benchmark Editor: View and export checks - Benchmark Editor: Activate benchmarks
PA Benchmark Editor	- Benchmark Editor: Create, delete and import checks - Benchmark Editor: Create, delete, modify and import benchmarks - Benchmark Editor: Create, delete and apply labels - Benchmark Editor: Edit benchmark tailoring
PA Viewer	- Benchmark Editor: View and export benchmarks - Benchmark Editor: View and export checks - Policy Auditor: View Audits and Assignments - Policy Auditor: View Waivers - Policy Auditor Agent: View settings
PA Waiver Granter	- Benchmark Editor: View and export benchmarks - Benchmark Editor: View and export checks

Permission Set	Permissions
	• Issue Management: Create, edit, view and purge assigned issues • Policy Auditor: View Audits and Assignments • Policy Auditor: Grant and modify Waivers

Policy Auditor Agent Plug-in

The McAfee Policy Auditor Agent Plug-in is responsible for updating the audit schedule and launching audit scans as required. The Agent Plug-in determines the age of the current information and uses any pending blackout or whiteout windows to determine if and when content should be re-evaluated.

Editing server settings

Use this task to edit the Policy Auditor server settings.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Configuration | Server Settings**.
- 2 Select **Policy Auditor** under **Setting Categories**. The Policy Auditor server settings appear in the right panel.
- 3 Click **Edit**. The **Edit Policy Auditor** page appears.
- 4 Change the settings to the values that you want. Click **Save**.

Managing Policy Auditor permission sets

Use these tasks to manage Policy Auditor permission sets.

Tasks

- ▶ [Creating a permission set](#)
- ▶ [Duplicating a permission set](#)
- ▶ [Editing a permission set](#)
- ▶ [Deleting a permission set](#)

Creating a permission set

Use this task to create a Policy Auditor permission set.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Configuration | Permission Sets**, then click **New Permission Set**. The **New Permission Set** page appears.
- 2 Type a **Name** for the permission set, such as **Policy Auditor Editor** and select the **Users** to which the set is assigned.
- 3 Click **Save**. The **Permission Sets** page appears.
- 4 Select the new permission set. Information about the selection appears in the details pane.
- 5 Click **Edit** next to the Policy Auditor section. The **Edit Permission Set** page appears.
- 6 Select the appropriate options, then click **Save**.
- 7 Repeat for all sections of the permission set for which you want to grant permissions.

Duplicating a permission set

Use this task to duplicate Policy Auditor permission sets.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Configuration | Permission Sets**, then select the Policy Auditor permission set that you want to edit in the **Permission Sets** list. Its details appear to the right.
- 2 Click **Duplicate**, type a **New name** in the **Action** pane, then click **OK**.
- 3 Select the new duplicate in the **Permission Sets** list. Its details appear to the right.
- 4 Click **Edit** next to any section for which you want to grant permissions.
- 5 On the **Edit Permission Set** page that appears, select the appropriate options, then click **Save**.
- 6 Repeat for all sections of the permission set for which you want to grant permissions.

Editing a permission set

Use this task to edit Policy Auditor permission sets.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Configuration | Permission Sets**, then select the Policy Auditor permission set that you want to edit in the **Permission Sets** list. The details pane shows the permission settings.

- 2 Click **edit** next to any section for which you want to grant permissions.
- 3 On the **Edit Permission Set** page that appears, select the appropriate options, then click **Save**.
- 4 Repeat for all sections of the permission set for which you want to grant permissions.

Deleting a permission set

Use this task to delete a Policy Auditor permission set.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Configuration | Permission Sets**, then select the Policy Auditor permission set that you want to delete in the **Permission Sets** list. Its details appear to the right.
- 2 Click **Delete**. The **Action** pane informs you whether any users are assigned to the permission set and gives you the opportunity to cancel the action.
- 3 Click **OK** in the **Action** pane. The permission set no longer appears in the **Permission Sets** list.

Complying with SCAP

Policy Auditor uses the Security Content Automation Protocol (SCAP) to perform automated audits, including policy compliance evaluations such as FISMA.

Contents

- ▶ [Statement of FDCC Compliance](#)
- ▶ [Statement of SCAP Implementation](#)
- ▶ [Statement of CVE Implementation](#)
- ▶ [Statement of CCE Implementation](#)
- ▶ [Statement of CPE Implementation](#)
- ▶ [Statement of CVSS Implementation](#)
- ▶ [Statement of XCCDF Implementation](#)
- ▶ [Statement of OVAL Implementation](#)

Statement of FDCC Compliance

McAfee asserts that Policy Auditor 5.0 does not alter or conflict with the Federal Desktop Core Configuration (FDCC) settings on Microsoft Windows XP and Vista systems.

Statement of SCAP Implementation

The Security Content Automation Protocol (SCAP) is a collection of six open standards developed jointly by various government organizations and the private sector. Security content conforming to the SCAP standard can be used by any product that supports the standard and the results can be shared between these products. This openness and standardization allows regulatory authorities and security administrators to construct more definitive security guidance and to reliably and repeatedly compare results.

McAfee Policy Auditor 5.0 was designed exclusively around SCAP. The product provides complete implementation of and support for all six SCAP standards. It uses the eXtensible Configuration Checklist Description Format (XCCDF) and Open Vulnerability and Assessment Language (OVAL) assessment protocols to determine what items to check on a system and how to check them. It uses the Common Vulnerabilities and Exposures (CVE), Common Configuration Enumeration (CCE), Common Platform Enumeration (CPE), and Common Vulnerability Scoring System (CVSS) reference protocols to ensure all rules are accurately and appropriately processed and the results properly shown in reports and export files.

Statement of CVE Implementation

McAfee Policy Auditor 5.0 fully implements and supports the Common Vulnerabilities and Exposures (CVE) standard vulnerability dictionary. CVE provides unique, standardized identifiers for security vulnerabilities. CVE does not address compliance items — only vulnerability issues. Each CVE identifier consists of a CVE identifier number, such as CVE-2008-0042; an indication of whether the CVE has a status of "entry" or "candidate;" a description of the vulnerability; and any references, such as advisories or OVAL identification.

The security content provided by McAfee refers to CVE identifiers when addressing vulnerabilities and whether a vendor's patch has been applied to address the vulnerability. Policy Auditor

Statement of CCE Implementation

McAfee Policy Auditor 5.0 fully implements and supports the Common Configuration Enumeration (CCE) standard.

While CVE identifies vulnerabilities, CCE uniquely identifies security-related configuration issues in a standard manner. CCE is designed to support software-based configurations, not hardware configurations. Further, if there are several ways to set a configuration, such as password length, CCE concentrates on the configuration itself, not the means by which that configuration was achieved.

CCE references in SCAP content allow Policy Auditor to compare configurations across systems and across single systems over a user-definable period of time.

Statement of CPE Implementation

McAfee Policy Auditor 5.0 fully implements the Common Platform Enumeration (CPE) standard.

CPE provides a standard reference and notation method to software and operating systems. For example, Windows XP is a structured naming scheme that is based upon the generic syntax for Uniform Resource Identifiers (URI). CPE provides the following:

- formal name format
- language for describing complex platforms
- method for checking names against a system
- description format for binding text and tests to a name

Policy Auditor allows users to create audits with SCAP content that covers a number of common Operating Systems and platforms. For example, an audit may cover both Windows XP and Windows Vista operating systems. By using CPE, Policy Auditor is able to use the correct SCAP content on the correct system.

Statement of CVSS Implementation

McAfee Policy Auditor 5.0 fully implements the Common Vulnerability Scoring System (CVSS). CVSS is a standardized open framework for measuring the impact of vulnerabilities. Each CVE includes an associated CVSS vector for use in determining the relative severity of vulnerabilities. CVSS is built upon a quantitative model that ensures repeatable measurements on systems, valid comparisons between systems, and allows users to view the underlying vulnerability

characteristics. Using CVSS weighted scores can help an organization determine and prioritize responses to detected vulnerabilities.

Policy Auditor supports all 4 standard SCAP scoring models. By default, it uses a Flat Unweighted scoring model normalized to 100. The scoring can be changed for comparison purposes.

Statement of XCCDF Implementation

McAfee Policy Auditor 5.0 provides complete implementation of version 1.4.1 of the eXtensible Configuration Checklist Description Format (XCCDF).

XCCDF supports the exchange of information, results document generation, tailoring, automated compliance testing, compliance scoring, and provides a data model and format for storing results of benchmark compliance testing. The goal of XCCDF is to provide a uniform standard for the expression of benchmarks and other configuration guidance to encourage good security practices.

Policy Auditor uses benchmarks from McAfee or third-party sources to construct audits. Users can select the benchmark profile, if any, to use for the audit. After a system is audited, the system agent returns the audit results to Policy Auditor, which analyzes and reports on the configuration and vulnerability data. The user specifies how long audit data is retained so that they or auditors can review any changes in the state of a system over time.

Statement of OVAL Implementation

McAfee Policy Auditor 5.0 fully implements and supports the Open Vulnerability and Assessment Language (OVAL).

OVAL is an international standard that promotes openly-available security content. It is the common language for security experts to check for the presence of vulnerabilities and configuration issues on computer systems. OVAL provides a structured model for network and system administrators to detect vulnerabilities and configuration issues on managed systems.

When a system is audited, the McAfee agent processes the OVAL content according to the information in the XCCDF benchmarks contained in the audit. The OVAL content captures the state of the system at the particular point in time that the audit is run. The results are returned to Policy Auditor for analysis and reporting. The user specifies how long audit data is to be retained so that they or auditors can review any changes in the state of a system over time.

Managing the Policy Auditor Agent Plug-in

The Policy Auditor Agent Plug-in is an extension of the McAfee agent. The extension manages the schedule for performing audits, runs the audits, and returns the results to Policy Auditor.

Are you deploying the McAfee Policy Auditor Agent Plug-in for the first time?

When installing and uninstalling the McAfee Policy Auditor Agent Plug-in for the first time:

- Understand that the Agent Plug-in can only be installed on systems that already have McAfee Agent 3.6 patch 2 or later installed
- Understand that the basic function of the Agent Plug-in is to run audits and relay the results back to Policy Auditor
- Know what platforms are supported and which of your systems is supported by the Agent Plug-in
- Understand how to deploy the Agent Plug-in
- Know how to verify that the task deploy the Agent Plug-in is running and when it is finished
- Understand how to verify that the Agent Plug-in is communicating with the server
- Understand how to uninstall the Agent Plug-in

Contents

- ▶ [The Policy Auditor Agent Plug-in and how it works](#)
- ▶ [Supported platforms](#)
- ▶ [Managing content](#)
- ▶ [Working with the McAfee Policy Auditor Agent Plug-in](#)

The Policy Auditor Agent Plug-in and how it works

The McAfee Policy Auditor Agent Plug-in is responsible for updating the audit schedule and launching audit scans per a schedule that you set. The Agent Plug-in determines the age of the current information and uses any pending blackout or whiteout windows to determine if and when content should be re-evaluated.

Upon receipt of a new audit, the plug-in calculates and persists the date and time of the next run. Upon completion of an audit, the plug-in calculates the date and time of the next run. The ePO server can request an immediate scan, in which case the plug-in marks the frequency information as expired, thus forcing a recalculation of the date and time for the next run. Existing whiteout and blackout windows are respected.

The Agent Plug-in is able to perform audits when a managed system is not connected to its network. Once the system is reconnected to the network, the Agent Plug-in returns the results to Policy Auditor.

Supported platforms

Policy Auditor 5.0 and the Policy Auditor Agent Plug-in supports the following platforms:

OS	X86	X64	Other Processors	Notes
Windows 2000 Server	X			
Windows 2000 Advanced Server	X			
Windows 2000 Professional	X			
Windows XP Professional	X	X		Native 32 and 64-bit Agent
Windows Server 2003 Standard Edition	X	X		Native 32 and 64-bit Agent
Windows Server 2003 Enterprise Edition	X	X		Native 32 and 64-bit Agent
Windows Vista	X	X		Native 32 and 64-bit Agent
Windows Server 2008	X	X		Native 32 and 64-bit Agent
Mac OS X 10.4	X	X	PowerPC (32/64-bit)	Universal binary
Mac OS X 10.5	X	X	PowerPC (32/64-bit)	Universal binary
HP-UX 11i v1			RISC	
HP-UX 11i v2			RISC	
Solaris 8			SPARC	
Solaris 9			SPARC	
Solaris 10			SPARC	
Red Hat Linux AS, ES, WS 4.0	X	X		32 -bit Agent on 64-bit H/W
Red Hat Enterprise Linux 5.0, 5.1	X	X		32 -bit Agent on 64-bit H/W

Managing content

Content for Policy Auditor consists of benchmarks and checks. This content package is included when the product is installed, and automatically loaded into the ePolicy Orchestrator master repository.

ePolicy Orchestrator has a default server task that updates the master repository from the McAfee update site that runs on a daily schedule. You should verify whether this task is enabled. If you want to update McAfee Policy Auditor content on a different schedule, create a new server task.

For information about repository management and server tasks, see the ePolicy Orchestrator documentation.

Working with the McAfee Policy Auditor Agent Plug-in

Use these tasks to manage the installation and uninstallation of the McAfee Policy Auditor Plug-in.

Tasks

- ▶ Sending manual wake-up calls to a group
- ▶ Deploying the Policy Auditor Agent Plug-in
- ▶ Determining whether the Agent Plug-in is being deployed
- ▶ Verifying that the Agent Plug-in has been deployed
- ▶ Verifying that the agent and server are communicating
- ▶ Uninstalling the Policy Auditor Agent Plug-in
- ▶ Determining whether the Agent Plug-in is being removed
- ▶ Verifying that the Agent Plug-in has been uninstalled

Sending manual wake-up calls to a group

Use this task to manually send an agent or SuperAgent wake-up call to a System Tree group. This is useful when you have made policy changes and you want agents to call in for an update.

Before you begin

Before sending the agent wake-up call to such a group, make sure that wake-up support for the group is enabled and applied on the **General** tab of the **McAfee Agent** policy pages (enabled by default).

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Systems | System Tree | Groups**, then select the group under **System Tree**.
- 2 Select **More Actions** at the bottom left of the page and select **Wake Up Agents**. The **Wake Up McAfeeAgent** page appears.
- 3 Verify that the group appears next to **Target group**.
- 4 Select whether to send the agent wake-up call to **All systems in this group** or to **All systems in this group and subgroups**.
- 5 Select whether to send an **Agent wake-up call** or **SuperAgent wake-up call** next to **Type**.
- 6 Accept the default or type a different **Randomization** (0 - 60 minutes). If you type 0, agents respond immediately.
- 7 During regular communication, the agent sends only properties that have changed since the last agent-server communication. This task is set by default to **Get full product properties**. To send the complete properties as a result of this wake-up call, ensure this is option selected.
- 8 Click **OK** to send the agent or SuperAgent wake-up call.

Deploying the Policy Auditor Agent Plug-in

Use this task to deploy the Policy Auditor Agent Plug-in to managed systems on your network.

Before you begin

- McAfee Agent 3.6 patch 2 or later must be installed on each system

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Systems | System Tree** and select the **Client Tasks** tab.
- 2 Click **New Task**.
- 3 Enter a name for the task and any descriptive text.
- 4 For the **Type** property, select **Product Deployment (McAfee Agent)** from the drop-down list. Click **Next**.
- 5 On the Configuration page:
 - a For **Target platforms**, select the target platform on which the agent plug-in will be deployed.
 - b For **Products and components**, select the proper McAfee Policy Auditor Agent from the drop-down list. The name of the agent must agree with the **Target Platforms** setting. For example, if you have selected Solaris as your target platform, you should select McAfee Policy Auditor Agent for Solaris 5.0.0 from **Products and Components**.
 - c Set the **Action** field to Install, and the **Language** field to English.
 - d If desired, you can set the **Run at every policy enforcement** option. Setting this assures that the Policy Auditor Agent Plug-in is always going to be on your managed systems, and prevents users from circumventing network security policy by removing it.
 - e Click **Next**.
- 6 On the Schedule page:
 - a For **Schedule status**, set Enabled or Disabled. You can later enable the task if you are not yet ready.
 - b For **Schedule type**, select when you want the task to run.
 - c For **Options**, check and set values for any of the three choices: stopping the task if too much time elapses, randomizing the task, and running the task again if it is missed.
 - d Set a start date and an end date for the task. If you set the **Run at every policy enforcement** option on the Configuration page, it is recommended you use the **No end date** option.
 - e Set whether to use the local system time or Coordinated Universal Time (UTC) for running the task.
 - f For **Schedule**, select an option from the drop-down list for how to run the task, and the desired time value or values. You can run the task once at a specific time, repeatedly between two times, or repeatedly starting at a specific time. If the Policy Auditor Agent Plug-in is already installed on a system, the task is skipped.
 - g For **Daily**, set how often (in number of days) you want the task to run.
 - h Click **Next**.
- 7 Review the task settings on the Summary page. Click **Save** to store the task, **Back** to make changes, or **Cancel**.

- 8 Send a manual wake-up call to the appropriate group if you want the task to run immediately.

Determining whether the Agent Plug-in is being deployed

Use this task to determine whether the Policy Auditor Agent Plug-in is being deployed to a system.

Before you begin

You must have a Policy Auditor Agent Plug-in install Client Task that is enabled and running.

Task

For option definitions, click ? in the interface.

- 1 Go to **Systems | System Tree** and select the **Systems** tab.
- 2 Select the group under **System Tree** containing the system you want to check. Select the system.
- 3 Select **More Actions** at the bottom left of the page and select **Show Agent Log**. A new browser window will open that shows the agent log.
- 4 Search the log for an entry like the following, where <Install PA Agent> is the name of the client task installing the Policy Auditor Agent Plug-in.
Scheduler: Invoking task [<Install PA Agent 1>]...

Verifying that the Agent Plug-in has been deployed

Use this task to determine whether the Policy Auditor Agent Plug-in has been deployed to a system.

Before you begin

You must have a Policy Auditor Agent Plug-in installation Client Task that has run.

Task

For option definitions, click ? in the interface.

- 1 Go to **Systems | System Tree** and select the **Systems** tab.
- 2 Select the group under **System Tree** containing the system you want to check. Select the system.
- 3 Select **More Actions** at the bottom left of the page and select **Show Agent Log**. A new browser window will open that shows the agent log.
- 4 Search the log for an entry like the following, where <Install PA Agent> is the name of the client task installing the Policy Auditor Agent Plug-in.
Scheduler: Task [<Install PA Agent>] is finished

Verifying that the agent and server are communicating

Use this task to determine whether the Policy Auditor Agent Plug-in and the server are communicating with each other.

Before you begin

You must have already installed the Policy Auditor Agent Plug-in on the systems for which you want to verify communication.

Task

For option definitions, click ? in the interface.

- 1 Send a manual wake-up call to the group containing the systems that you want to check.
- 2 Go to **Reporting | Audit Log**.
- 3 Search the log for an entry like the following:
Wake Up Agents | Succeeded

Uninstalling the Policy Auditor Agent Plug-in

Use this task to uninstall the Policy Auditor Agent Plug-in from managed systems on your network.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Systems | System Tree** and select the **Client Tasks** tab.
- 2 Click **New Task**.
- 3 Enter a name for the task and any descriptive text.
- 4 For the **Type** property, select **Product Deployment (McAfee Agent)** from the drop-down list. Click **Next**.
- 5 On the Configuration page:
 - a For **Target platforms**, select the target platform on which the agent plug-in will be deployed.
 - b For **Products and components**, select the proper McAfee Policy Auditor Agent from the drop-down list. The name of the agent must agree with the **Target Platforms** setting. For example, if you have selected Windows as your target platform, you should select McAfee Policy Auditor Agent for Windows 5.0.0 from **Products and Components**.
 - c Set the **Action** field to Remove, and the **Language** field to English.
 - d If desired, you can set the **Run at every policy enforcement** option. Setting this assures that the Policy Auditor Agent Plug-in will always be uninstalled from your managed systems.
 - e Click **Next**.
- 6 On the Schedule page:
 - a For **Schedule status**, set Enabled or Disabled. You can later enable the task if you are not yet ready.
 - b For **Schedule type**, select when you want the task to run.
 - c For **Options**, check and set values for any of the three choices: stopping the task if too much time elapses, randomizing the task, and running the task again if it is missed.
 - d Set a start date and an end date for the task. If you set the **Run at every policy enforcement** option on the Configuration page, it is recommended you use the **No end date** option.

- e Set whether to use the local system time or Coordinated Universal Time (UTC) for running the task.
 - f For **Schedule**, select an option from the dropdown list for how to run the task, and the desired time value or values. You can run the task once at a specific time, repeatedly between two times, or repeatedly starting at a specific time. If the Policy Auditor Agent Plug-in is already installed on a system, the task is skipped.
 - g For **Daily**, set how often (in number of days) you want the task to run.
 - h Click **Next**.
- 7 Review the task settings on the Summary page. Click **Save** to store the task, **Back** to make changes, or **Cancel**.
 - 8 Send a manual wake-up call to the appropriate group if you want the task to run immediately.

Determining whether the Agent Plug-in is being removed

Use this task to determine whether the Policy Auditor Agent Plug-in is being removed from a system.

Before you begin

You must have a Policy Auditor Agent Plug-in removal Client Task that is enabled and running.

Task

For option definitions, click ? in the interface.

- 1 Go to **Systems | System Tree** and select the **Systems** tab.
- 2 Select the group under **System Tree** containing the system you want to check. Select the system.
- 3 Select **More Actions** at the bottom left of the page and select **Show Agent Log**. A new browser window will open that shows the agent log.
- 4 Search the log for an entry like the following, where <Remove PA Agent> is the name of the client task uninstalling the Policy Auditor Agent Plug-in.
Scheduler: Invoking task [<Remove PA Agent>]...

Verifying that the Agent Plug-in has been uninstalled

Use this task to determine whether the Policy Auditor Agent Plug-in has been removed from a system.

Before you begin

You must have a Policy Auditor Agent Plug-in removal Client Task that has run.

Task

For option definitions, click ? in the interface.

- 1 Go to **Systems | System Tree** and select the **Systems** tab.
- 2 Select the group under **System Tree** containing the system you want to check. Select the system.

- 3** Select **More Actions** at the bottom left of the page and select **Show Agent Log**. A new browser window will open that shows the agent log.
- 4** Search the log for an entry like the following, where <Remove PA Agent> is the name of the client task uninstalling the Policy Auditor Agent Plug-in.
Scheduler: Task [<Remove PA Agent>] is finished

Creating and Managing Audits

McAfee Policy Auditor 5.0 makes it easy to demonstrate and report on compliance with recognized corporate and industry security standards. You can create your audits from a McAfee-supplied selection of predefined benchmarks established by government and industry such as SOX, HIPPPAA, PCI, and FISMA. You can also customize your own audits, then determine which managed systems pose a risk.

Are you creating or managing audits for the first time?

When creating and managing audits for the first time:

- Understand what audits are and how they work
- Understand the considerations for including and excluding systems in your audits
- Know how benchmark profiles work and how to choose a profile for your audit
- Learn how benchmark labels can help you create audits
- Understand audit frequency and how the McAfee Policy Auditor Agent Plug-in uses it to help determine when to run an audit
- Understand whiteout and blackout periods and how the McAfee Policy Auditor Agent Plug-in uses them to help determine when to run an audit
- Learn how to create a new audit and to edit an existing audit
- Understand how to export XCCDF and OVAL audit results

The Audits Tab

The **Audits** tab is a repository for all of your audits. You can view the **Audits** tab by going to **Systems | Audits**. The **Audits** panel shows you the following information about each of your audits:

Column	Definition
Audit Name	The human-readable name given to the audit
Description	A description of what the audit does and what operating systems or software that it targets.
frequency	Denotes how long the results are valid
Created On	The creation date of the audit
Created By	The user who created the audit
Last Modified On	The date when the audit was last modified
Last Modified By	The user who last modified the audit

The **Audits** tab also contains buttons to help you manage your audits.

Option	Definition
New Audit	Create a new audit using the New Audit Builder
Delete	Delete the selected audits
Export OVAL	Creates an OVAL results file that conforms to the OVAL results schema. This file can be consumed by any tool that understands the OVAL results schema. For example, Remediation Manager 4.5 can import OVAL results.
View Results	View the audit results for a selected timeframe
Edit Audit	Edit an existing audit
Export XCCDF	Creates a file that conforms to the XCCDF results schema, as defined in the XCCDF specification. It contains the latest results for all of the systems and benchmarks in the audit. The results file can be consumed by any tool that understands the XCCDF results schema.

Contents

- ▶ Audits and how they work
- ▶ Considerations for including systems in an audit
- ▶ Benchmark profiles and their impact on managed systems
- ▶ Benchmark labels and how they can aid in creating audits
- ▶ Audit frequency
- ▶ Audit whiteout and blackout periods
- ▶ How viewing audit results works
- ▶ Audit exports
- ▶ Setting whiteout and blackout periods
- ▶ Exporting audits to XCCDF
- ▶ Exporting audits to OVAL
- ▶ Creating a new audit
- ▶ Deleting Audits

Audits and how they work

An audit gathers data about managed systems to determine whether they are in compliance with corporate and industry security standards. An audit consists of:

- A benchmark or a selected profile within a benchmark
- Managed Systems
- A frequency (how often the data should be gathered)

Benchmarks contain rules describing the desired state of a managed system according to recognized standards.

Policy Audit

[-] Benchmarks	(XCCDF)
[-] Profiles	(XCCDF) - Optional
[-] Groups	(XCCDF)
[-] Rules	(XCCDF / OVAL)
[-] Checks	(OVAL)
[-] Values	(XCCDF)
[+] Systems / Groups / Devices	(ePO System Tree)
[+] Audit Frequency	(PA 5)
[+] Waivers	(PA 5) - Optional

Figure 2: Policy Tree

Rules contain one or more checks written in the OVAL language.

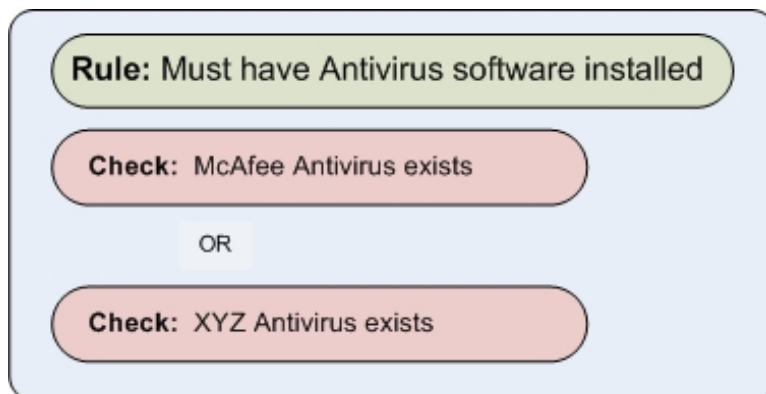


Figure 3: Example Rule

When you run an audit against a managed system, the audit reports the configuration status of the system compared with the rules in the benchmarks. When the default audit scoring model is used, the audit also reports a comparative score of the system ranging from 0 to 100.

Considerations for including systems in an audit

Audits are frequently designed for a specific computer system configuration, and Policy Auditor allows you to include or exclude systems from an audit based on a number of system characteristics.

How including systems works

Policy Auditor provides two methods for including systems in an audit. The first method allows you to include managed systems by specifying **System Tree and Tags**:

- **Add System** — a managed system as defined by system name, IP address, MAC address, or user name

- **Add Group** — a group defined in the ePO System Tree
- **Add Tag** — systems that have been tagged in the ePO System Tree, such as server, workstation, or laptop

The second method allows you to include managed systems by specifying **Criteria**. Criteria can be defined by selecting properties and using comparison operators and values to represent managed systems. You can select one or more of the following properties:

- CPU Serial Number
- CPU Type
- CPU Speed
- Default Language
- Description
- DNS Name
- Domain Name
- Free Disk Space (MB)
- Free Memory (bytes)
- IP Address
- IPX Address
- Is 64 bit OS
- Is Laptop
- MAC Address
- Number of CPUs
- OS Build Number
- OS OEM Identifier
- OS Platform
- OS Service Pack Version
- OS Type
- OS Version
- Subnet Address
- Subnet Mask
- System Name
- Time Zone
- Total Disk Space (MB)
- Total Physical Memory (bytes)
- User Name
- Up to 4 use-defined properties

How excluding systems works

Policy Auditor allows you to exclude one or more managed systems based system name, IP address, MAC address, or user name

Benchmark profiles and their impact on managed systems

Audits have benchmarks assigned to them. Many benchmarks contain profiles, which are named sets of selected groups, rules, and valued targeted toward different computer system configurations and threat risks. A profile can:

- Enable or disable one or more groups
- Enable or disable one or more rules
- Change the variables that are used within a rule, such as the minimum password length

Profiles are normally designed to apply to a particular set of systems. For example, a benchmark could contain two profiles, one for Windows and one for UNIX. Alternatively, a benchmark might contain "High Security", "Medium Security", and "Low Security" profiles.

Selecting a profile should be based upon the risk of the systems being audited. Systems containing customer credit card information pose more of a threat to an organization if the data is compromised than does a machine used to create company newsletters.

Benchmark labels and how they can aid in creating audits

Labels provide a method for classifying a benchmark for aid in searches. Each benchmark can have zero or more labels attached to it. Labels can describe the programmatic usage of a benchmark, such as applying a label of MNAC to a benchmark designed for the McAfee Network Access System extension. Labels can also describe the functionality of a benchmark, such as applying a label of SOX to a benchmark designed to test compliance with Sarbanes-Oxley standard. Labels are applied with the Benchmark Editor extension or are contained in McAfee-supplied benchmarks.

When creating or editing an audit, the benchmark selection process provides a dropdown box showing all of the available benchmark labels. This tool allows you to filter benchmarks based on the label that you wish to use for your audit.

Audit frequency

Frequency defines how often data should be gathered. It is defined as "Audit results should be no older than *nnn* time unit", where "*nnn*" is a number and "time unit" is "days", "weeks", "months," or "years." For example, if the frequency for an audit is defined as 1 month and a managed system has not been audited in more than 1 month, the system is out of frequency and its status is unknown .

Audit whiteout and blackout periods

Audit whiteout periods are times when an audit may run on a system or group of systems. Audit blackout periods are times when an audit may not be run.

Audits are not scheduled. For example, consider a benchmark that was last evaluated at 5:14 pm on Sunday May 6th. The frequency requirement states the information should not be older

than 4 days. Blackout windows are set from 8am to 5pm on weekdays. Whiteout windows cover the remaining period.

If the benchmark is scheduled for re-evaluation during the Thursday evening whiteout window, the frequency requirement of 4 days would be calculated so the benchmark must be evaluated no later than Thursday morning.

How viewing audit results works

Policy Auditor offers a number of options for viewing audit results. You can view whether a particular benchmark has passed, failed, or exhibited unknown results. Several options are available for viewing system and rule compliance.

Results timeframe control

The **Results timeframe** control allows you to view the results of an audit at any point in time since the audit first began. By default, the calendar is set to **Today**, which shows the results for current systems as defined by the frequency settings. A checkbox is available to show the last valid results if today's results are not current. Finally, the calendar control allows you to pick a date in the past and see the audit results for that date.

Audit Benchmarks pane

The **Audit Benchmarks** pane shows the status of each benchmark in the audit. You can view the following columns in the pane:

- **Benchmark ID** — Benchmark identifier
- **Profile ID** — Profile identifier, if any
- **Pass** — the number of benchmarks for which all systems passed the audit
- **Fail** — the number of benchmarks for which all systems failed the audit
- **Unknown** — the number of benchmarks which, for some reason, were not audited

You can click on the hyperlinked number in the **Pass**, **Fail**, and **Unknown** columns to take you to the **View System Results** page.

View System Results Column

Under the **View Results** column, clicking **systems** allows you to view the results for each system audited. This is an extension of the **Audit Results** pane that allows you to see the results at the system level. The following columns appear in the **Benchmark Systems** pane:

- **Audit Date** — the date of the audit being viewed
- **Expiration Date** — the expiration date, if any, of the audit
- **Score** — the audit score for the system
- **System Group** — the name of the group, if any, that the system belongs to
- **System Name** — the name of the system
- **System Tags** — any tags associated with the system
- **Rules Passed** — the number of rules which passed the audit
- **Rules Failed** — the number of rules which failed the audit
- **Rules Other** — the number of systems which, for some reason, were not audited

The page provides a control that allows you to view the results by system group, system subgroup, systems with a specific tag, or even individual systems.

You can also adjust the results timeframe to select an audit to review.

View Rule Results Column

Under the **View Results** column, clicking **rule** allows you to view the rule results for each system audited. This is an extension of the **Audit Results** pane that it allows you to see the results at the rule level. The following columns appear in the **Benchmark Rules** pane:

- **Rule ID** — the benchmark rule identifier
- **Group Path** — the path of the group containing the rule
- **Systems Passed** — the number of systems which passed the audit
- **Systems Failed** — the number of systems which failed the audit
- **Systems Other** — the number of systems which, for some reason, were not audited

The page provides a control that allows you to view the results by benchmark rule group, benchmark rule subgroup, or a specific rule which can be selected by clicking the **Find** button and selecting a rule.

You can also adjust the results timeframe to select an audit to review.

Audit exports

Audits and audit results may be exported in two different formats: XCCDF and OVAL. In each case, the information is saved as a ZIP file. Common uses for exporting audits is for transfer to another ePO server or for use in a third-party application.

Export XCCDF creates a file that conforms to the XCCDF results schema, as defined in the XCCDF specification. It contains the latest results for all of the systems and benchmarks in the audit. The results file could be consumed by any tool that understands the XCCDF results schema.

Export OVAL creates an OVAL results file that conforms to the OVAL results schema. This file can be consumed by any tool that understands the OVAL results schema. For example, Remediation Manager 4.5 can import OVAL results.

Setting whiteout and blackout periods

Use this task to set whiteout and blackout periods for audits.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Systems | System Tree** and select the **Policies** tab.
- 2 Select Policy Auditor 5.0 from the **Product** drop-down box.
- 3 Under the **Policy** column, select My Default. The whiteout/blackout page appears.

- 4 To block out a period of time when audits should not run, click a white square corresponding to your desired day and hour. To allow a period of time when an audit should be able to run, click a blue square corresponding to your desired day and hour.
- 5 Click **Save**.

Exporting audits to XCCDF

Use this task to export an audit to a file that conforms to the XCCDF results schema, saved as a ZIP file.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Systems | Audits**.
- 2 Select the audits you wish to export to the XCCDF format and click **Export XCCDF**. The **File Download** dialog appears.
- 3 Click **Save**. The **Save As** dialog appears.
- 4 Give the export ZIP file an appropriate name and click **Save**.

Exporting audits to OVAL

Use this task to export an audit to a file that conforms to the OVAL results schema, saved as a ZIP file.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Systems | Audits**.
- 2 Select the audits you wish to export to the OVAL format and click **Export OVAL**. The **File Download** dialog appears.
- 3 Click **Save**. The **Save As** dialog appears.
- 4 Give the export ZIP file an appropriate name and click **Save**.

Creating a new audit

Use these tasks to create a new audit.

Tasks

- ▶ [Selecting benchmarks](#)
- ▶ [Deleting Audits](#)

Selecting benchmarks

Use this task to select one or more benchmarks for use in an audit. If a benchmark has profiles, you can choose to use one of the profiles in the audit or simply use the base benchmark.

Before you begin

You must have appropriate permissions to perform this task.

Only benchmarks activated by Benchmark Editor are available for selection. For many users, McAfee-supplied benchmarks can be used as is. Users with special needs can tailor McAfee-supplied benchmarks and edit third-party benchmarks.

NOTE: To activate benchmarks, go to **Systems | Benchmarks**, select one or more benchmarks, and click **activate**.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Systems | Audits**. The **Audits tab** appears.
- 2 Click **New Audit**. The **Select Benchmarks** page of the **New Audit Builder** appears.
- 3 Click the **Label** drop-down box and select a label that matches the type of audit that you wish to create. For example, select the FISMA label and all benchmarks related to FISMA will appear in the **activated Benchmarks** section.
- 4 In the **activated Benchmarks** section, scroll through the filtered benchmarks and select one or more benchmarks that you wish to appear in your audit. Click **Add Benchmark**.
- 5 In the **Selected Benchmarks** section, click select profile to choose the profile that you wish to use in your audit. Note that some benchmarks do not have any profiles.
- 6 If you decide that you do not wish to use one or more of the benchmarks in the **Selected Benchmarks** section, click **remove**.
- 7 Click **Next**. The **Select Systems** page appears.

Selecting systems

Use this task to select which managed systems you want to audit.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Select a method to add systems to the audit.
 - a Select **System Tree and Tags** and click one or more of **Add System**, **Add Group**, or **Add Tab** to add systems to the audit.

- b** Select **Criteria**, then select one or more **Available Properties** to add to the **Computer Properties** pane. Choose the **Comparison** and select or type in the value.
- 2** If you wish to exclude systems from the audit, click **Add System** under the **Exclude these** pane.
- 3** Click **Next**. The **Define frequency** page appears.

Defining frequency

Use this task to stipulate the frequency for an audit. Defining frequency tells Policy Auditor that the audit results must not be older than a specified number of days, weeks, or months.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

- 1** In **Results must not be older than**, type a number in the text box and select **Days**, **Weeks**, or **Months** in the drop-down box.
- 2** Click **Next**. The **General** page appears.

Naming and describing your audits

Use this task to name and describe your existing audits.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

- 1** Type in an appropriate name and description for the audit.
- 2** Click **Next**. The **Summary** page appears.

Saving your audit

Use this task to save your new audit.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

- 1** Review your new audit. If changes need to be made, click **Back** until you have reached the appropriate page.
- 2** Click **Save**.

Editing existing audits

Use these tasks to edit existing audits. Editing audits is useful in a number of situations, for example:

- The groups or systems in your organization changes
- You wish to select a different profile for a benchmark
- The frequency needs to be changed

Tasks

- ▶ [Selecting benchmarks for existing audits](#)
- ▶ [Selecting systems for existing audits](#)
- ▶ [Defining frequency for existing audits](#)
- ▶ [Naming and describing your audits](#)
- ▶ [Saving your existing audits](#)

Selecting benchmarks for existing audits

Use this task to select one or more benchmarks for use in an existing audit.

Before you begin

You must have appropriate permissions to perform this task.

You must have benchmarks that have been activated by Benchmark Editor. For the overwhelming number of users, McAfee-supplied benchmarks can be used as is. Go to **Systems | Benchmarks**, select benchmarks that are in the received state, and click **activate**. Users with special needs can tailor McAfee-supplied benchmarks and edit third-party benchmarks.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Systems | Audits**. The **Audits tab** appears.
- 2 Click **New Audit**. The **Select Benchmarks** page of the **New Audit Builder** appears.
- 3 Click the **Label** drop-down box and select a label that matches the type of audit that you wish to create. For example, select the FISMA label and all benchmarks related to FISMA will appear in the **activated Benchmarks** section.
- 4 In the **activated Benchmarks** section, scroll through the filtered benchmarks and select one or more benchmarks that you wish to appear in your audit. Click **Add Benchmark**.
- 5 In the **Selected Benchmarks** section, click **select profile** to choose the profile that you wish to use in your audit. Note that some benchmarks do not have any profiles.
- 6 If you decide that you do not wish to use one or more of the benchmarks in the **Selected Benchmarks** section, click **remove**.
- 7 Click **Next**. The **Select Systems** page appears.

Selecting systems for existing audits

Use this task to select which managed systems you want to audit.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Select a method to add systems to the audit.
 - a Select **System Tree and Tags** and click one or more of **Add System**, **Add Group**, or **Add Tab** to add systems to the audit.
 - b Select **Criteria**, then select one or more **Available Properties** to add to the **Computer Properties** pane. Choose the **Comparison** and select or type in the value.
- 2 If you wish to exclude systems from the audit, click **Add System** under the **Exclude these** pane.
- 3 Click **Next**. The **Define Frequency** page appears.

Defining frequency for existing audits

Use this task to stipulate the frequency for an audit. Defining frequency tells Policy Auditor that the audit results must not be older than a specified number of days, weeks, or months.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 In **Results must not be older than**, type a number in the text box and select **Days**, **Weeks**, or **Months** in the drop-down box.
- 2 Click **Next**. The **General** page appears.

Naming and describing your audits

Use this task to name and describe your existing audits.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Type in an appropriate name and description for the audit.
- 2 Click **Next**. The **Summary** page appears.

Saving your existing audits

Use this task to save your existing audits.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Review your new audit. If changes need to be made, click **Back** until you have reached the appropriate page.
- 2 Click **Save**.

Deleting Audits

Use this task to delete an existing audit.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Systems | Audits**.
- 2 Select the audits you wish to delete and click **Delete**. Click **OK** in the **Action Panel**.

Scoring Audits

When Policy Auditor performs an audit on a managed system, it accepts as input the state of the system and any benchmarks in the audit, and produces several types of output, including a human-readable report about compliance that includes the compliance score and a listing of which rules passed and which failed on the system.

Policy Auditor supports all of the scoring models described in the XCCDF 1.1.4 specifications. When Policy Auditor performs an audit, it uses any of the score computation models designated by the user.

Are you scoring audits for the first time?

When scoring audits for the first time:

- Understand the different types of scoring models and how they work
- Understand how to change a scoring audit to fit your organizational needs

Contents

- ▶ [Score computation algorithms](#)
- ▶ [Changing the scoring model](#)

Score computation algorithms

Policy Auditor provides you with the means to score audits according to four different scoring models. McAfee Policy Auditor uses the flat unweighted scoring model normalized to a value of 100 as its default scoring model.

Default scoring model

While the default scoring model is the default for XCCDF, Policy Auditor uses the flat unweighted scoring model normalized to 100. While the other scoring models can be useful and are supported, the model used by McAfee allows easy and meaningful comparison between audits on managed systems.

In the default model, computation of the score is performed independently for each collection of subgroups and rules in each group, and then for each rule and group within the benchmark. The final test score is the normalized score value on the benchmark object.

Flat scoring model

The flat scoring model computes the sum of the weights for the rules that passed as the score, and the sum of the weights of all applicable rules as the maximum possible score. Though this

model is easy to determine and to understand, scores between different managed systems may not be directly comparable because the maximum score can vary.

For example, assume that the rules in a benchmark are not weighted. If Managed System A passes 40 of the rules in an audit and the maximum possible score can be obtained by passing 50 rules, then the score, expressed as a percentage, is 80%. If Managed System B passes 40 of the weighted rules in the same audit and the maximum possible score can be obtained by passing 80 weighted rules, then the score, expressed as a percentage, is 50%. Though each managed system passed the same number of rules, the scores are different because the maximum possible scores are different for each machine. Though the lack of weighted rules make the scores for both managed systems comparable, the presence of weighted rules would skew the scores and it would be difficult to compare the results.

Flat unweighted scoring model

McAfee Policy Auditor uses the flat unweighted scoring model normalized to a value of 100 as its default scoring model.

The flat unweighted scoring model computes the sum of the rules that passed as the score, and the sum of all applicable rules as the maximum possible score. Because weighting is not taken into account, scores between different managed systems can be easily compared.

Absolute scoring model

The Absolute Scoring Model yields a score of 100 when the managed system passes all applicable rules. If all applicable rules do not pass, the system is assigned a score of 0.

Changing the scoring model

Use this task to change the scoring model for audit results. When you change the scoring model, the score automatically recalculates according to the model chosen.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Go to **Configuration | Server Settings**.
- 2 Select **Policy Auditor** under **Setting Categories**. The Policy Auditor server settings appear in the right panel.
- 3 Click **Edit**. The **Edit Policy Auditor** page appears.
- 4 Select the scoring model that you want from the **Default Scoring Model** drop-down box. Click **Save**.

Creating and Managing Waivers

Waivers provide a way for you to temporarily affect audit scoring for managed systems. Waivers are useful when you have a managed system that is non-compliant with a rule or a benchmark but you do not wish to bring the system into compliance for a temporary period. An example of this would be a system in the Accounting Department that you don't want to patch systems near the end of an accounting cycle. You can create a waiver that will temporarily ignore any issues on the machine until the critical time has passed.

Are you creating and managing waivers for the first time?

When creating and managing waivers for the first time:

- Understand what waivers are and how they work
- Understand that waivers are temporary
- Familiarize yourself with the 3 different types of waivers and how they differ from one another
- Understand waiver status
- Understand the concept of start dates and expire dates
- Learn how to filter waivers
- Learn how to request a waiver
- Learn how to grant waivers and understand the permission set that one needs to be able to grant waivers
- Understand how to expire and delete waivers and the difference expiring and deleting waivers

Contents

- ▶ [How waivers work](#)
- ▶ [Waivers catalog](#)
- ▶ [Types of waivers](#)
- ▶ [Waiver status](#)
- ▶ [Waiver benchmark and rule management](#)
- ▶ [How start dates and expires dates work](#)
- ▶ [Filtering waivers](#)
- ▶ [Requesting waivers](#)
- ▶ [Granting waivers](#)
- ▶ [Expiring waivers](#)
- ▶ [Deleting waivers](#)

How waivers work

Waivers temporarily affect audit scoring for managed systems. Policy Auditor provides three types of waivers with each one exhibiting different functionality. Waivers only appear on the **Waivers** tab when a user with the proper permissions grants approval for the waiver to take effect. Depending upon the internal security policies of your organization, the persons who request waivers and the persons who grant them may be different people. However, a person who has the permissions to grant waivers may request a waiver and grant it from the same screen.

Policy Auditor waivers provide a way for you to:

- Bypass auditing a system
- Force the result of a benchmark rule to be Pass. This potentially alters the benchmark score of a system
- Exclude the result of a benchmark rule, thus altering the benchmark score of a system

Setting	Description
Waiver Name	A name that you give to a waiver. The name does not have to be unique.
Waiver Type	The three types of waivers are Exception, Exemption, and Suppression.
System	The system to which the waiver applies. Each waiver can only be assigned to only one system.
Benchmark	You are required to assign a benchmark to Exception and Suppression waivers. Exemption waivers are system-based and, when you request a waiver, Policy Auditor does not allow you to assign a benchmark to them.
Rule	You are required to assign a rule to Exemption and Suppression waivers. The list of rules is automatically generated when you select an active benchmark.
Start date	The date when a waiver takes effect
Expires	The date when a waiver is no longer in effect
Notes	Descriptive information about the waiver
Status	A waiver may have a status of Requested, Upcoming, In-effect, or Expired.
Granted by	The name of the user who grants, or enables, a waiver

Waivers catalog

The **Waivers Catalog** is shown in the bottom pane of the **Waivers** tab. The catalog allows you to view the various properties of your waivers. You can select the properties you want to view by clicking **Options**, then **Choose Columns**. From there, you can choose the columns that you want to view in the catalog.

Column	Description
Actions	The View action appears under the Actions column. Depending upon the status of the waiver and your permissions, you may Expire or Delete a waiver by clicking View .
Benchmark	You are required to assign a benchmark to Exception and Suppression waivers. Exemption waivers are system-based only and, when you request a waiver, you cannot assign a benchmark and a rule to them.
End Date	The date when a waiver is no longer in effect
Rule	You are required to assign a rule to Exemption and Suppression waivers. The list of rules is automatically generated when you select an active benchmark.

Column	Description
Start Date	The date when a waiver takes effect
Status	A waiver may have a status of Requested, Upcoming, In-effect, or Expired.
System	The system to which the waiver applies. Each waiver is assigned to only one system.
System Group	The System Tree group to which the system belongs
Waiver Name	A name that you give to a waiver. The name does not have to be unique.
Waiver Type	The three types of waivers are Exception, Exemption, and Suppression.

Types of waivers

Policy Auditor provides three types of waivers that apply to a system being audited. Each type of waiver has different effects on scoring results.

Exception waivers

Exception waivers force the result of a benchmark rule to be Pass, thus potentially altering the benchmark score of a system. They have the following characteristics:

- Each waiver applies only to a single managed system. Exception waivers require you to select a benchmark and a rule contained in the benchmark that will not apply to an audit of the system.
- The selected benchmark and rule is included in an audit of the system, but the audit result of the particular rule is always Pass.
- Only benchmarks that are Active can be specified in the waiver.
- Exception waivers can be backdated. Scores for any results collected during the backdate time frame are recalculated.
- Rules used in an exception waiver appear in the audit results.
- Example of scoring impact:

A benchmark has 5 rules. An audit is run and 4 rules pass and 1 fail, resulting in a score of 80%. If the rule that failed is granted an exception, then all 4 rules pass and the score is 100%.

Exemption waivers

Exemption waivers are system-based and prevent a system from being audited. When you request an Exemption waiver, Policy Auditor does not allow you to assign a benchmark and rule. They have the following characteristics:

- Each waiver applies only to a single managed system. Exemption waivers do not require you to select a benchmark and a rule for the system.
- A system is not audited while the waiver is in effect.
- An exemption waiver can be created at any time for an existing system.
- An exemption waiver cannot be backdated.
- A system affected by an exemption waiver will not appear in the audit results.

- Example of scoring impact:
A benchmark has 5 rules. An audit is run on a system and 4 rules pass and 1 fail, resulting in a score of 80%. If the system is granted an exemption waiver, that system does not appear in the scoring.

Suppression waivers

Suppression waivers allow a rule to be included in an audit, but excludes the result, thus altering the benchmark score of a system. Suppression waivers have the following characteristics

- Each waiver applies only to a single managed system. Suppression waivers require you to select a benchmark and a rule.
- The benchmark's rule is included when the system is audited.
- Rule audit results are not included in the score.
- Only benchmarks that are Active can be specified in the waiver.
- Suppression waivers cannot be backdated.
- Rules used in an suppression waiver do not appear in the scoring for a system.
- Rules used in an suppression waiver appear in the audit results.
- Example of scoring impact:
A benchmark has 5 rules. An audit is run and 4 rules pass and 1 fail, resulting in a score of 80%. If the rule that failed is granted a suppression waiver, then the score is 80%.

Waiver status

Waivers can have the following status properties:

Status	Description
Requested	A waiver has been requested but approval has not been granted for it to take effect. Requested waivers do not appear on the Waivers tab but appear in the Issue Catalog (go to Reporting Issues). Requested waivers can be deleted.
Upcoming	A waiver has been requested and granted approval but the waiver is not in effect because the start date has not yet arrived. Upcoming waivers can be deleted.
In-effect	The waiver is active and audits involving the system specified by the waiver will temporarily affect the scoring of the system. In-effect waivers cannot be deleted.
Expired	The waiver is no longer in effect, either by user intervention or because the expires date has arrived. Expired waivers cannot be deleted.

Waiver benchmark and rule management

Exception and Suppression waivers require that you assign a benchmark and rule to them. These types of waivers are both rule-based and system based. Exemption waivers are

system-based only and, when you request a waiver, Policy Auditor does not allow you to assign a benchmark and rule.

Waivers can only be applied to a single system.

When you request a waiver and select a benchmark, the rules applying to that benchmark are automatically populated in the **Rule** drop-down box. When you select a rule, it is assigned to that waiver. Any audit using that benchmark and rule will adjust the scoring appropriately according to the type of waiver.

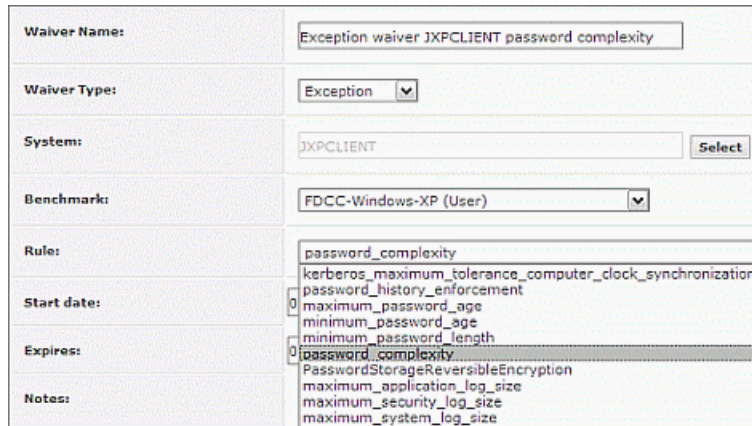


Figure 4: Selecting a rule for a waiver

How start dates and expires dates work

Waivers are effective for a limited time only. You specify a Start Date and an Expires Date when you create the waiver.

The Start Date is when the waiver takes effect. The Expires Date is when the waiver is no longer in effect. The Start Date is inclusive while the Expires Date is not inclusive. For example, if you set a Start Date of 12/01/08 and an Expires Date of 01/01/09, then the waiver applies to audit results acquired on 12/01/08 through 12/31/08. An audit conducted on 01/01/09 will not be affected by the waiver.

Because of how Start Dates and Expires Dates work, the Expires date must be at least one day ahead of the Start Date.

Filtering waivers

Use this task to filter waivers. Policy Auditor provides three ways for you to filter waivers, all of which work together in tandem:

Filter	Description
Status	Show all waivers in the Waiver Catalog or select filters according to their status of In-effect, Expired, or Upcoming.
As of	Use the calendar control to select a date and the Waiver Catalog changes to show the status of each waiver as of the selected date.
Filter	When you select This Group Only , Policy Auditor displays waivers only applying to managed systems in the selected

Filter	Description
	group of the System Tree . When you select This Group and all Subgroups , Policy Auditor shows waivers in the selected group of the System Tree as well as all subgroups of the selected group.

Tasks

- ▶ Filtering waivers by status
- ▶ Filtering waivers as of a specified date
- ▶ Filtering waivers by group

Filtering waivers by status

Use this task to filter waivers in the **Waiver Catalog** by status.

Before you begin

Task

For option definitions, click ? in the interface.

- 1 Go to **Systems | Waivers**. The **Waivers** tab appears.
- 2 Select a group from the **System Tree** containing waivers of different status.
- 3 Use the **Status** drop-down list to select a status. Policy Auditor filters the **Waiver Catalog** according to the choice you make with the Status drop-down list.

Filtering waivers as of a specified date

Use this task to filter waivers according to a date that you select.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Go to **Systems | Waivers**. The **Waivers** tab appears.
- 2 Use the calendar control next to **As of** to select a different date. The **Waiver Catalog** changes to show the status of each waiver as of the selected date.

Example of filtering waivers according to a specified date

Assume the following:

- 1 Today's date is 10/01/2008.
- 2 Waiver A has a Start date of 11/01/2008 and an Expires date of 12/01/2008.
- 3 Waiver B has a Start date of 11/15/2008 and an Expires date of 12/16/2008.

As of today's date of 10/01/2008, Waiver A and Waiver B both have a status of Upcoming. Use the calendar control to reset the **As of** date to 12/02/2008. The **Waivers Catalog** shows the following.

- 1 Waiver A has a status of Expired.
- 2 Waiver B has a status of In-effect.

Use the calendar control to reset the **As of** date to 01/01/2009. The **Waivers Catalog** shows the following.

- 1 Waiver A has a status of Expired.
- 2 Waiver B has a status of Expired.

Click **Today** next to the **As of** date. The date is reset to today's date of 10/01/2008. The **Waivers Catalog** shows the following.

- 1 Waiver A has a status of Upcoming.
- 2 Waiver B has a status of Upcoming.

Filtering waivers by group

Use this task to filter waivers according to the group selected in the **System Tree**.

Before you begin

You must have appropriate permissions to perform this task. You must also have a group with waivers and a subgroup to that group that also contains waivers.

Task

For option definitions, click **?** in the interface.

- 1 Go to **Systems | Waivers**. The **Waivers** tab appears.
- 2 Select the group containing the waivers from the **System Tree**. The Waivers Catalog shows only the waivers for managed systems in the selected group.
- 3 Select **This Group Only** from the **Filter** drop-down list. The Waivers Catalog shows only the waivers for managed systems in the selected group.
- 4 Select **This Group and all Subgroups** from the **Filter** drop-down list. The **Waivers Catalog** shows the waivers for managed systems in the selected group and all the subgroups to the selected group.

Requesting waivers

Use this task to request any of the three types of waivers.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Systems | Waivers**. The **Waivers** tab appears.

- 2 Click **New Waiver**. The **Waiver Request** page appears.
- 3 Name the waiver then select the type of waiver that you wish to create from the **Waiver Type** drop-down list.
- 4 Click **Select**. The **Quick System Search** dialog appears.
- 5 Type the system name, IP address, MAC address, or user name that you wish to search for. If you do not know the full name or address, you can type in a partial search, like 172.21. Click **OK**. The **Search Results** page appears.
- 6 Select the system that you want the waiver to apply to. The **Search Results** page closes and the **Waiver Request** page appears.
- 7 Select the benchmark and rule that apply to the waiver. Exemption waivers do not require a benchmark and a rule.
- 8 Use the calendar control next to the **Start Date** and an **Expires Date** to select dates for the waiver to be in effect. The < and the > controls move the month backwards and forwards, respectively, while the << and the >> controls move the year backwards and forwards.
- 9 Type descriptive information that you want to associate with the waiver in the **Notes** box.
- 10 Click **Request Waiver**. The **Waivers** tab appears. The requested waiver does not appear in the **Waivers** tab because the waiver had not been granted yet. Requested waivers appear in the **Issues Catalog (Reporting | Issues)**. If you have permissions to grant waivers, you can click **Grant Waiver** and the waiver will appear in the **Waivers** tab.

Granting waivers

Use this task to grant approval for requested waivers.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Reporting | Issues**.

Issues			
	Name	Type	Description ▼
☐	Exempt max pw age f...	Request Waiver	Exemption waiver of maxim...
☐	Exception waiver DEV ...	Request Waiver	Exception waiver for DEV m...

Figure 5: Granting a waiver

- 2 Select a requested waiver and click **Edit**. The **Edit Issue** page will appear.
- 3 Click **Grant Waiver**, then **Cancel**. The waiver has been granted approval, has been removed from the **Issues Catalog**, and now appears in the **Waivers Catalog**.

Expiring waivers

Use this task to make a waiver expire.

Before you begin

You must have waiver grantor permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Systems | Waivers**. The **Waivers** tab appears.
- 2 Select a waiver that has the status of In-effect and click **View**.
- 3 Click **Expire Waiver**. The **Waivers** tab appears and the status of the waiver is Expired.

Deleting waivers

Use this task to delete a waiver.

Before you begin

You must have waiver grantor permissions to perform this task.

Policy Auditor places the following limits on deleting waivers:

- You can only delete waivers with the status of Upcoming or Requested.
- You cannot delete waivers with the status of In-effect or Expired.

Task

For option definitions, click ? in the interface.

- 1 Go to **Systems | Waivers**. The **Waivers** tab appears.
- 2 Select a waiver that has the status of Upcoming and click **View**.
- 3 Click **Delete Waiver**. The deleted waiver no longer appears in the **Waiver Catalog**.

Managing Issues and Tickets

The Issue extension allows you to create, modify, assign, and track issues. You can also add tickets to issues for tracking in a ticketing server.

Are you working with issues or tickets for the first time?

When working with issues and tickets for the first time:

- Understand what issues are and how they work.
- Ensure users have permissions to work with issues.
- To add tickets to issues:
 - Understand tickets and how they work with issues.
 - Install the extension for your ticketing server.
 - Register and configure your ticketing server.

Contents

- ▶ [Issues and how they work](#)
- ▶ [Tickets and how they work](#)
- ▶ [Integrations with ticketing servers](#)
- ▶ [Working with issues](#)
- ▶ [Working with ticketing servers](#)
- ▶ [Working with tickets](#)

Issues and how they work

Issues are action items, which can be prioritized, assigned, and tracked. Issues can also be associated with tickets in a ticketing server.

How issues are created

Issues can be created manually or automatically by the system in response to certain events or conditions. These events and conditions can be predefined by other product extensions and by user-configured responses within those products. For example, an issue might be created automatically if a noncompliant system is discovered during an audit.

The Issue extension has a basic issue type. However, other product extensions can have their own issue types as well.

How issues are managed

How issues are managed and their life cycles are defined by the user and the installed product extensions. An issue's state, priority, severity, resolution, due date, and assignee are all user-defined, and can be changed any time. If the Automatic Response extension is installed, defaults for these can also be specified. The defaults are automatically applied whenever an issue is created based on a user-configured response. Responses also allow events to be aggregated into a single issue.

Issues can be deleted manually, and closed issues can be purged based on their age manually and automatically through a user-configured server task.

NOTE: Editing, deleting, and purging issues with tickets will affect their association. For more details, see the section of this guide about tickets and how they work.

Tickets and how they work

A ticket is the external equivalent of an issue that exists in a ticketing server. Once a ticket is added to an issue, the issue is referred to as a "ticketed issue."

How tickets are created

A ticket can be added to an issue manually or automatically by the system. An issue (ticketed issue) can have only one associated ticket.

When a ticket is added to an issue, the state of the resulting ticketed issue is changed to Ticketed, regardless of the issue's status prior to being ticketed. When the ticket is created in the ticketing server, that ticket's ID is added to the ticketed issue. The ticket ID creates the ticket-to-issue association.

After the steps for integrating a ticketing server are completed, tickets will be created for all subsequent issues automatically. You must add tickets manually to any issues that existed prior to the integration.

How ticketed issues are assigned

Adding an assignee manually to a ticketed issue breaks the issue-to-ticket association because it is considered editing the issue. Therefore, you should add an assignee to an issue before the ticket is added. Do this by specifying an assignee in the response, which creates issues. In this way, an assignee is added to the issue automatically when it is created. For details, see the section in this guide about creating issues automatically with responses.

How tickets and ticketed issues are closed

Ticketed issues are closed automatically by the system when the server task, which synchronizes ticketed issues, runs. This server task identifies the tickets that changed to the Closed state since the last time the task ran. The status of a ticketed issue associated with a closed ticket is then changed to Closed. Also, that ticket's comments replace the comments in the ticketed issue if the integration of the ticketing server was configured to overwrite ticketed issue comments. For details, see the section in this guide about ticket and issue comments.

Why ticketed issues should not be edited manually

Editing a ticketed issue manually breaks the relationship between the ticketed issue and the ticket. Therefore, you should update the associated ticket in the ticketing server. For example, if you close a ticketed issue manually or add an assignee, the issue-to-ticket association is broken and the server task, which synchronizes ticketed issues, cannot retrieve the ticket's state or comments.

If you delete a ticketed issue, the associated ticket remains in the ticketing server. This ticket cannot be re-associated with another issue.

Adding a comment to a ticketed issue does not break the issue-to-ticket association because it is not considered editing the issue. For details, see the section in this guide about ticket and issue comments.

How comments are handled

When a comment is added to a ticketed issue, it is added to the associated ticket immediately or the next time the server task, which synchronizes ticketed issues, runs. Ticketed issue comments are only added to tickets that are not in the Closed state.

If the ticketing server's mapping is configured to allow issue comments to be overwritten by ticket comments, when a ticket's state becomes Closed, comments for that ticket replace all of the comments in the associated ticketed issue. This process is performed when the server task, which synchronizes ticketed issues, identifies a ticket whose state changed to Closed since the last time the task was run. This task is performed only once for each closed ticket. Allowing issue comments to be overwritten by ticket comments can give users that have access to the system, but not to the ticketing server, the ability to see what happened to the ticket.

How tickets are reopened

Reopening a ticket does not reopen the associated ticketed issue. When a ticket is added to a previously ticketed issue with a ticket ID that can be matched to a ticket in the ticketing server, then that ticket is reopened. If the ticket ID cannot be matched, a new ticket is created. The configuration mapping for the ticketing server must also be configured to allow tickets to be reopened. For more details, see the section in this guide about configuring the mapping for ticketing servers.

How ticketed issues are synchronized

The Issue extension includes the Issue Synchronization server task, which synchronizes ticketed issues with their associated tickets in the ticketing server. This server task is disabled by default. Therefore, it will not run on schedule until enabled. When this server task runs, the system attempts to:

- Change the status of ticketed issues from Ticketed to Closed if the state of their associated tickets is closed.
- Create tickets for issues or add comments to tickets that the system was unable to create or add previously. For example, if there was a communication error when the tickets or the comments were first added.
- Replace the comments of a ticketed issue with the comments of its associated ticket if the ticket's state is Closed, and the integration of the ticketing server was configured to overwrite ticketed issue comments.

- If the registered server for the ticketing server is deleted, the system changes the state of each ticketed issue to Assigned or to New if the ticketed issue does not have an assignee specified.

Integrations with ticketing servers

The integration of a ticketing server allows the system to force the creation of tickets associated with issues that were created in product extensions. The following ticketing servers are supported:

- Hewlett-Packard Openview Service Desk versions 4.5 and 5.1
- BMC Remedy Action Request System versions 6.3 and 7.0

The person who performs this integration should be familiar with the ticketing server and its fields and forms. Integrating a ticketing server consists of these basic steps:

- 1 Install the extension for the ticketing server.

NOTE: The system running the ticketing extension must be able to resolve the address of the Service Desk system. This might involve adding the IP address of the Service Desk system to the hosts file on the system running the ticketing extension, or setting up a domain trust between the two systems. For more details, see the section in this guide about configuring DNS for a Service Desk 4.5 integration.

- 2 Add a registered server for the ticketing server. Only one registered ticketing server can exist at a time.
- 3 Configure the field mappings between issues and tickets.

Considerations when deleting a registered ticketing server

There might be times when you want to delete the registered server for your ticketing server. For example, if you upgrade your ticketing server. When the registered server is deleted, the system changes the state of each ticketed issue to Assigned or to New if the ticketed issue does not have an assignee specified. The system only performs this action when the server task, which synchronizes ticketed issues, runs. This is why it is important to disable that server task if you are upgrading the ticketing server. For more details, see the section in this guide about upgrading registered ticketing servers.

When the registered ticketing server is deleted, the ticket ID that associated the ticket to the ticketed issue remains with that ticketed issue. This allows the ticket to be reopened if the issue-to-ticket association is broken. For example, if the server task, which synchronizes ticketed issues, runs before the upgraded server is registered. For more details, see the sections in this guide about upgrading a ticketing server and about how tickets are reopened.

Required fields for mapping

To determine which ticket fields must be mapped, review the fields on the desired ticket form that are required for a ticket to be created within the ticketing server. For information about which fields are required for your ticket form, see the documentation for your ticketing server.

For the system to know when to close ticketed issues, the field with the ticket's state must be mapped. If you want ticket comments added to ticketed issues, the ticket's comment field must be mapped in addition to the ticket's state field.

Sample mappings

When you register your ticketing server, you must also configure the field mappings for issues and tickets. These sample field mappings are provided for reference only. Your mappings will vary based on the fields required in your ticketing server and the values those fields will accept.

Sample mapping for Remedy

This sample mapping is for reference only.

NOTE: Source values, mapped values, and field IDs are case-sensitive.

Map Issue to Ticket

- **Ticket form:** Help Desk
- **Ticket field:** 8
 - **Operation:** Identity
 - **Source field:** Name
- **Ticket field:** 7
 - **Operation:** Substitution
 - **Source field:** State
 - **Values:** **Default Value:** 0

Source Value	Mapped Value
NEW	0
RESOLVED	2
ASSIGNED	1

- **Ticket field:** 2
 - **Operation:** Custom Mapping
 - **Source field:** Type the user name for the ticketing server. This is the same user name provided for Authentication on the Description page of the Registered Server Builder.
- **Ticket field:** 200000004
 - **Operation:** Custom Mapping
 - **Source field:** External

TIP: In this example, "External" is used to specify that the ticket was created by a product external to the ticketing server. If you want to know which product created the ticket, type the name of the product instead.

- **Ticket field:** 240000008

NOTE: Remedy servers can have multiple comment or diary fields. Make sure to choose the one you want used for this integration. If a comment field is not mapped, then ticketed issue comments cannot be added to tickets.

- **Operation:** Identity
- **Source field:** Activity Log
- **Ticket field:** Type the name or ID for any open text field

- **Operation:** Identity
- **Source field:** URL

Map Ticket back to Issue Status field

NOTE: Because this section only maps the ticket's state/status, you are not prompted to add the ID of the issue's status (state) field. This field is implied.

- **Operation:** Substitution
- **Source field:** 7
- **Values: Default Value:** 0

Source Value	Mapped Value
4	CLOSED

- **Overwrite issue comments with ticket comments:** selected
- **Ticket Comment field:** 240000008
- **Tickets can be re-opened:** selected

Sample mapping for Service Desk

This sample mapping is for reference only.

NOTE: Source values, mapped values, and field IDs are case-sensitive.

Map Issue to Ticket

- **Ticket form:** Default_Problem
- **Ticket field:** Description
 - **Operation:** Identity
 - **Source field:** Name
- **Ticket field:** Status
 - **Operation:** Substitution
 - **Source field:** State
 - **Values: Default Value:** 10

Source Value	Mapped Value
NEW	10
RESOLVED	20
UNKNOWN	20
ASSIGNED	20

- **Ticket field:** Information
 - **Operation:** Identity
 - **Source field:** Description
- **Ticket field:** HistoryLines
 - **Operation:** Identity

- **Source field:** Activity Log
- **Ticket field:** Type the name or ID for any open text field
 - **Operation:** Identity
 - **Source field:** URL

Map Ticket back to Issue Status field

NOTE: Because this section only maps the ticket's state/status, you are not prompted to add the ID of the issue's status (state) field. This field is implied.

- **Operation:** Substitution
- **Source field:** Status
- **Values: Default Value:** TICKETED

Source Value	Mapped Value
40	CLOSED

- **Overwrite issue comments with ticket comments:** selected
- **Ticket Comment field:** HistoryLines
- **Tickets can be re-opened:** selected

Working with issues

Use these tasks to create and manage issues.

Tasks

- ▶ [Creating issues](#)
- ▶ [Creating issues automatically with responses](#)
- ▶ [Assigning issues](#)
- ▶ [Viewing the details of issues](#)
- ▶ [Adding comments to issues](#)
- ▶ [Editing issues](#)
- ▶ [Deleting issues](#)
- ▶ [Purging closed issues](#)
- ▶ [Purging closed issues on a schedule](#)

Creating issues

Use this task to create an issue. If you registered a ticketing server, a ticket is also created for the issue automatically. However, only data for fields that were mapped in the ticketing server configuration are written to the ticket.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Reporting | Issues**, then click **New Issue**.

- 2 In the **Action** panel, select an issue type, then click **OK**. This choice determines the options available on the New Issue page.
- 3 Type a name and description for the issue.
- 4 Accept the default values for state, priority, severity, and resolution, or select different values.
- 5 Optionally, type the user name of the user to whom you want the issue assigned. The assignee must have a user account in the system.
- 6 Optionally, select a due date and time for the issue.
- 7 Provide any additional information based on the issue type selected.
- 8 Click **Save**.

Creating issues automatically with responses

Use this task to configure responses that create issues automatically.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Automation | Responses**, then click **New Response**. The Description page of the Response Builder appears.
- 2 Type a name and description for the server task.
- 3 Select an event group and type.
- 4 Enable or disable the response. If you disable the response, it does not run until it is enabled.
- 5 Click **Next**. The Filter page appears.
- 6 Select properties to narrow which events trigger the response. Selected properties appear in the content pane with operators to specify criteria that narrows the data returned for that property.
- 7 Click **Next**. The Aggregation page appears.
- 8 Next to **Aggregation**, select **Trigger this response for every event**, or **Trigger this response if multiple events occur within** a defined amount of time. If you select the latter, define this amount of time in minutes, hours, or days.
- 9 If you selected **Trigger this response if multiple events occur within**, you can choose to send a response **When the number of events is at least** a defined number of events.
- 10 Next to **Grouping**, select **Do not group aggregated events**, or **Group aggregated events by** a property of the event. If you select the latter, select an event property.
- 11 Click **Next**. The Actions page appears.
- 12 Select **Create issue** from the drop-down list.
- 13 Select the type of issue to create. This choice determines the options available on this page.
- 14 Type a name and description for the issue. Optionally, select one or more variables to insert for the name and description.

- 15 Accept the default values for state, priority, severity, and resolution, or select different values.
- 16 Type the name of the user to whom you want the issue assigned. The assignee must have a user account in the system.
- 17 Provide any additional information based on the issue type selected.
- 18 Click **Next**. The Summary page appears.
- 19 Review the details for the response, then click **Save**.

Assigning issues

Use this task to assign a single issue, or multiple issues at once. An issue can also be assigned during its creation and when editing or viewing its details.

NOTE: Adding an assignee to a ticketed issue breaks the association between the ticketed issue and the ticket. Therefore, ticketed issues are skipped. For details, see the section in this guide about how ticketed issues are assigned.

Task

- 1 Go to **Reporting | Issues**, select checkbox next to each issue you want, then click **Assign to user**.
- 2 In the **Action** panel, type the user name of the user to whom you want the issues assigned. The assignee must have a user account in the system or the issues cannot be assigned.
- 3 Click **OK** to assign the non-ticketed issues selected.

Viewing the details of issues

Use this task to view the details of an issue, including the activity log. An issue can also be edited, assigned, deleted, and a comment or ticket added from this page.

Task

For option definitions, click **?** on the page displaying the options.

- Go to **Reporting | Issues**, then click an issue. The Issue Details page appears.

Adding comments to issues

Use this task to add a comment to a single issue or to multiple issues at once. A comment can be added to an issue in a similar way when viewing the details of an issue. If this is a ticketed issue, the comment is also be added to the ticket.

The history of comments added to an issue is displayed on the Issue Details page.

Task

- 1 Go to **Reporting | Issues**, select the checkbox next to each issue you want, then click **Add comment**.
- 2 In the **Action** panel, type the comment you want added to the selected issues.
- 3 Click **OK** to add the comment.

Editing issues

Use this task to edit an issue. An issue can be edited in a similar way when viewing its details.

CAUTION: Editing a ticketed issue breaks the association between the ticketed issue and the ticket.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Reporting | Issues**, select the checkbox next to the issue, then click **Edit**.
- 2 Edit the issue as needed.
- 3 Click **Save**.

Deleting issues

Use this task to delete a single issue, or multiple issues at once. An issue can be deleted in a similar way when viewing its details. Deleting a ticketed issue deletes the issue, but the associated ticket remains in the ticketing server.

Task

- 1 Go to **Reporting | Issues**, select the checkbox next to each issue you want, then click **Delete**.
- 2 In the **Action** panel, click **OK** to delete the issues selected.

Purging closed issues

Use this task to purge all closed issues from the database. Purging closed issues deletes them permanently. Purging a closed ticketed issue deletes the issue, but the associated ticket remains in the ticketing server.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Reporting | Issues**, then click **Purge**.
- 2 In the **Action** panel, type a number, then select a time unit.
- 3 Click **OK** to delete closed issues older than the specified date permanently.

NOTE: This function affects all closed issues; not just those in the current view.

Purging closed issues on a schedule

Use this task to purge closed issues with a scheduled server task. Purging closed issues deletes them permanently. Purging a closed ticketed issue deletes the issue, but the associated ticket remains in the ticketing server.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Automation | Server Tasks**, then click **New Task**. The Description page of the Server Task Builder appears.
- 2 Type a name and description for the server task.
- 3 Enable or disable the schedule for the server task. If you disable the schedule, the server task does not run until it is enabled.
- 4 Click **Next**. The Actions page appears.
- 5 Select **Purge Closed Issues** from the drop-down list.
- 6 Type a number, then select a time unit.
- 7 Click **Next**. The Schedule page appears.
- 8 Schedule the server task, then click **Next**. The Summary page appears.
- 9 Review the details of the server task, then click **Save**.

Working with ticketing servers

Use these tasks to integrate your ticketing server.

Tasks

- ▶ [Installing extensions for ticketing servers](#)
- ▶ [Registering and mapping a ticketing server](#)
- ▶ [Upgrading a registered ticketing server](#)

Installing extensions for ticketing servers

Use these tasks to install the ticketing extension for your ticketing server.

Tasks

- ▶ [Stopping and starting the server](#)
- ▶ [Copying the Remedy files](#)
- ▶ [Copying the Service Desk files](#)
- ▶ [Installing the ticketing server extensions](#)

Stopping and starting the server

Use this task to stop the McAfee Policy Auditor Application server running on a Microsoft Windows system. The server must be stopped before the required files for the ticketing server can be copied. After the files are copied, start the server.

Task

- 1 Go to **Start | Control Panel | Administrative Tools**, then double-click **Services**.
- 2 In the **Name** column, locate then double-click **McAfee Policy Auditor Application Server**.

- 3 Select the **General** tab.
- 4 Under **Service status**, click **Stop**. The server is now stopped.
- 5 Copy the required files for your ticketing server, then repeat steps 1-3.
- 6 Under **Service status**, click **Start**. The server is now running.

Copying the Remedy files

Use this task to copy the files required for the Remedy extension. For information about these files, see your Remedy documentation. The Remedy extension includes support for the Remedy 6.3 and 7.0 servers.

NOTE: You can use the Remedy 5.1 or 7.0 API files for the Remedy extension. McAfee does not support an integration with the Remedy 5.1 server, but the 5.1 API files will work for integrations with the Remedy 6.3 or 7.0 servers. However, the Remedy 6.3 API files are not supported.

Before you begin

- Stop the server.
- If using the Remedy 5.1 API files, locate these required files to copy:
 - arapi51.dll
 - arjni51.dll
 - arrpc51.dll
 - arutil51.dll
 - arapi51.jar
 - arutil51.jar
- If using the Remedy 7.0 API files, locate these required files to copy:
 - arapi70.dll
 - arjni70.dll
 - arrpc70.dll
 - arutiljni70.dll
 - arutil70.dll
 - arxmlutil70.dll
 - icudt32.dll
 - icuin32.dll
 - icuuc32.dll
 - arapi70.jar
 - arutil70.jar

Task

- 1 Copy these required files to the \Server\bin folder of your Policy Auditor installation. For example, C:\Program Files\McAfee\ePolicy Orchestrator\Server\bin.
 - If using the Remedy 5.1 API files:
 - arapi51.dll
 - arjni51.dll

- arrpc51.dll
 - arutil51.dll
 - If using the Remedy 7.0 API files:
 - arapi70.dll
 - arjni70.dll
 - arrpc70.dll
 - arutiljni70.dll
 - arutil70.dll
 - arxmlutil70.dll
 - icudt32.dll
 - icuin32.dll
 - icuuc32.dll
- 2** Copy these required files to the Server\common\lib folder of your Policy Auditor installation. For example, C:\Program Files\McAfee\ePolicy Orchestrator\Server\common\lib.
- If using the Remedy 5.1 API files:
 - arapi51.jar
 - arutil51.jar
 - If using the Remedy 7.0 API files:
 - arapi70.jar
 - arutil70.jar

Copying the Service Desk files

Use this task to copy the files required for the Service Desk 5.1 or Service Desk 4.5 extension. For information about these files, see your Service Desk documentation.

Before you begin

- Stop the server.
- If using Service Desk 5.1, locate these required files to copy:
 - OvObsCommon-05.10.090.jar
 - OvObsSDK-05.10.090.jar
 - OvObsWebApi-Client-05.10.090.jar
 - OvObsWebApi-Common-05.10.090.jar
 - sd-webapi-05.10.090.jar
 - xpl-05.10.090.jar
- If using Service Desk 4.5, locate this required file to copy:
 - sd-webapi-4.5.0588.2205.jar

Task

- Copy the required files to the Server\common\lib folder of your Policy Auditor installation. For example, C:\Program Files\McAfee\ePolicy Orchestrator\Server\common\lib.

Installing the ticketing server extensions

Use this task to install ticketing server extensions.

Before you begin

- Copy the files required for the ticketing server.
- Restart the server.

Task

- 1 Go to **Configuration | Extensions**, then click **Install Extension**.
- 2 Browse to and select the extension (ZIP) file.
 - For Remedy, select Remedy.zip. This file includes support for Remedy 6.3 and 7.0.
 - For Service Desk 4.5, select ServiceDesk_4_5.zip.
 - For Service Desk 5.1, select ServiceDesk_5_1.zip.
- 3 Click **OK**.

Registering and mapping a ticketing server

Use these tasks to register and map a ticketing server. You must complete these tasks before tickets can be added to issues. Only one registered ticketing server can exist at a time.

Before you begin

Install the extension for your ticketing server.

Tasks

- ▶ [Configuring the DNS for Service Desk 4.5](#)
- ▶ [Registering a ticketing server](#)
- ▶ [Configuring the field mappings](#)

Configuring the DNS for Service Desk 4.5

Use this task to configure DNS for a Service Desk 4.5 integration. The system running the ticketing extension must be able to resolve the address of the Service Desk system.

Task

- Do one of the following:
 - On the system running the ticketing extension, edit your hosts file to include the IP address of the system running Service Desk 4.5, followed by a space, followed by the DNS suffix (the name of the system on which Service Desk 4.5 is running), then reboot the system running the ticketing extension. For example, in the file c:\windows\system32\drivers\etc\hosts file, add: 168.212.226.204 SRVDSK45.qaad.com

- On the system running Service Desk 4.5, add the name of that system as a DNS suffix in the IP settings, then reboot the Service Desk 4.5 system.

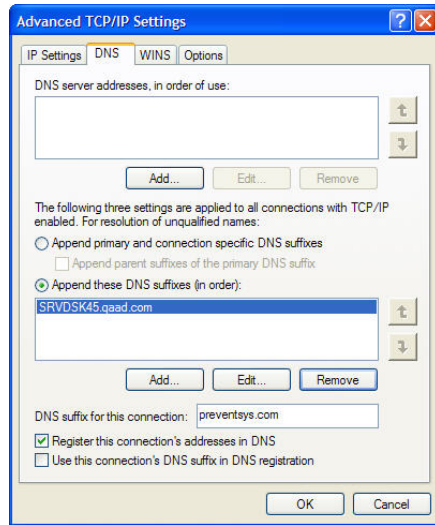


Figure 6: Example of settings for Service Desk 4.5 DNS

Registering a ticketing server

Use this task to register a ticketing server. This task must be completed before tickets can be associated with issues.

Before you begin

- Make sure you have installed the extension for your ticketing server.
- You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Network | Registered Servers**, then click **New Server**. The Description page of the Registered Server Builder appears.
- 2 Select the server type for your ticketing server. This choice determines the options available on subsequent pages of the builder.
- 3 Type a name and description, then click **Next**. The Details page appears.
- 4 Type the host for the server.
- 5 Type the port, user name, and password for the server.
- 6 If Service Desk 4.5 or 5.1 was selected, select a **Workflow**.

Configuring the field mappings

Use these tasks to configure the field mappings for a ticketing server. You must complete these tasks before tickets can be associated to issues.

Before you begin

- The ticketing server you want to configure must be running.

- Know which fields from the ticketing server need to be mapped.

Tasks

- ▶ [Mapping issues to tickets](#)
- ▶ [Mapping tickets back to issue status](#)

Mapping issues to tickets

Use this task to configure the field mapping from the issue to the ticket.

Task

For option definitions, click **?** on the page displaying the options.

NOTE: Source values, mapped values, and field IDs are case-sensitive.

- 1 Next to **Configure mapping**, click **Configure**. The Mapping page appears.
- 2 Select the options from the **Mapping Options** pane as needed. Selected options appear in the Mapping Definitions pane with operators to specify how an issue should be mapped to a ticket, and how a ticket should be mapped back to an issue. Both mappings must be completed.
- 3 Under **Map Issue to Ticket**, type the name of a **Ticket form**.
- 4 Type a **Ticket field ID**.
- 5 Select an **Operation**.
- 6 Do one of the following:
 - If **Substitution** is selected, select an issue field in the **Source field** drop-down list, then click **Edit** next to **Values**. The Edit Substitution Mapping dialog box appears.
 - 1 Type a **Default Value** that should be substituted if a source value, which is not mapped, is returned.
 - 2 Type a **Source Value** for the issue, then type the **Mapped Value** that should be substituted for this value in the ticket.
 - 3 Click **+** to map another value.
 - 4 When finished, click **OK**.
 - If **Numeric Range** is selected, select an issue field to map in the **Source field** drop-down list, then click **Edit** next to **Values**. The Edit Numeric Range Mapping dialog box appears.
 - 1 Type a **Default Value** that should be substituted if a source range, that is not mapped, is returned.
 - 2 Type the **Source Range** for the issue, then type the **Mapped Value** that should be substituted for this range in the ticket.
 - 3 Click **+** to map another value.
 - 4 When finished, click **OK**.
 - If **Custom Mapping** is selected, type the **Value** that should be added to the ticket.
- 7 Click **+** to map another ticket field.

Mapping tickets back to issue status

Use this task to configure the field mapping from the ticket back to the issue's status (state) field.

NOTE: Because this section only maps the ticket's state/status, you are not prompted to add the ID of the issue's status (state) field. This field is implied.

Task

For option definitions, click **?** on the page displaying the options.

NOTE: Source values, mapped values, and field IDs are case-sensitive.

- 1** Under **Map Ticket back to Issue Status field**, select an **Operation**.
- 2** In the **Source field**, type the ID of the ticket field that contains the state/status of the ticket.
- 3** If **Numeric Range** or **Substitution** is selected for the **Operation**, click **Edit** next to **Values**. A dialog box appears.
 - If **Numeric Range** is selected, type a range of **Ticket Values** for the ticket, then type the **Label** that is substituted for this range in the issue.
 - If **Substitution** is selected, type a **Source Value** for the ticket, then type the **Mapped Value** that is substituted for this value in the issue.
- 4** Select the checkbox if you want to **Overwrite issue comments with ticket comments**, then type the ID of the **Ticket comment field** that overwrites the data in the issue's comment field.
- 5** Select the checkbox if **Tickets can be re-opened**.
- 6** When finished, click **Test Mapping**.
- 7** If the test is successful, a ticket ID appears in a dialog box. This is the ID for a test ticket, which was created in your ticketing server. Locate this ticket in your ticketing server, and verify that all the values for the basic issue type are mapped correctly, including the test's comments.

NOTE: The test mapping function verifies the mapping for the basic issue type, regardless of the issue type configured. Therefore, testing the mapping for issue types from other product extensions (extended issue types) can be successful per the basic mapping test, but you might see unexpected results in the tickets. For these issue types, verify that tickets added to issues after your ticketing server is fully integrated are created correctly.

- 8** Click **OK**.
- 9** If the test was unsuccessful, review your mappings and the status of the ticketing server.
- 10** When finished testing the mapping, click **Save**. The Details page of the Registered Server Builder appears.

NOTE: You can save the configuration and register the server even if the mapping test fails.

- 11** When finished, click **Save**.

Upgrading a registered ticketing server

Use this task to modify the integration of the existing ticketing server if your ticketing server is upgraded.

Before you begin

- Make sure the upgraded version of the ticketing server is running.

Task

CAUTION: If the server task, which synchronizes ticketed issues, runs after the existing registered ticketing server is modified or deleted, but before the upgraded ticketing server is integrated, the issue-to-ticket association is broken. If this occurs, complete this task, then manually add tickets to all previously ticketed issues. This causes the reopen function to run. For more details, see the section in this guide about how tickets are reopened.

- 1 Do the following to disable the server task, which synchronizes ticketed issues.
 - a Go to **Automation | Server Tasks**, then click the issue synchronization server task. The Description page of the Server Task Builder appears.
 - b Select **Disable** next to **Schedule status**.
 - c Click **Save**.
- 2 Ensure that no instances of the server task are running. If an instance is running, wait for it to complete or cancel it before continuing.
- 3 Do one of the following:
 - Edit the existing registered ticketing server based on the configuration requirements for the upgraded ticketing server.
 - Delete the existing registered ticketing server, then create a new one based on the configuration requirements for the upgraded ticketing server.For more details, see the sections in this guide about integrating ticketing servers, installing ticketing server extensions, and registering and configuring a ticketing server.
- 4 After you have configured the integration with the upgraded ticketing server, enable the server task, which synchronizes ticketed issues.

Working with tickets

Use these tasks to add tickets to issues and to synchronize ticketed issues with the Issue Synchronization server task.

Tasks

- ▶ [Adding tickets to issues](#)
- ▶ [Synchronizing ticketed issues](#)
- ▶ [Synchronizing ticketed issues on a schedule](#)

Adding tickets to issues

Use this task to add a ticket to a single issue, or to add tickets to multiple issues at once. A ticket can be added in a similar way when viewing the details of an issue. When a ticket is added, a new ticket is created automatically in the ticketing server. Issues with existing tickets are ignored.

Before you begin

Make sure you have integrated a ticketing server.

Task

- 1 Go to **Reporting | Issues**, select the checkbox next to each issue, then click **Add ticket**.
- 2 In the **Action** panel, click **OK** to add a ticket to each selected issue.

Synchronizing ticketed issues

Use this task to run the Issue Synchronization server task, which updates ticketed issues and their associated tickets in the ticketing server.

Before you begin

Make sure you have integrated a ticketing server.

Task

For option definitions, click **?** on the pages displaying the options.

- 1 Go to **Automation | Server Tasks**.
- 2 Click **Run** next to the **Issue synchronization** task. The Server Task Log page appears.
- 3 Review the results of the server task. For more details, see the section in this guide about the server task log.

Synchronizing ticketed issues on a schedule

The Issue Synchronization server task updates ticketed issues and their associated tickets in the ticketing server. Use this task to configure the Issue Synchronization server task to run on a schedule.

NOTE: The schedule for the Issue Synchronization server task is disabled by default.

Before you begin

- You must have permissions to run server tasks and to purge issues to perform this task.
- Make sure you have integrated a ticketing server.

Task

For option definitions, click **?** on the pages displaying the options.

- 1 Go to **Automation | Server Tasks**, then click **Edit** in the **Actions** column for the **Issue synchronization** task. The Description page of the Server Task Builder appears.
- 2 Select **Enable** next to **Schedule status**. If you disable the schedule, the server task will not run on a schedule, but you can still run it manually.
- 3 Click **Next**. The Actions page appears.
- 4 Click **Next**. The Schedule page appears.
- 5 Schedule the server task as needed, then click **Next**. The Summary page appears.
- 6 Review the details of the server task, then click **Save**.

Querying the Database

Policy Auditor ships with its own querying and reporting capabilities. These are highly customizable and provide flexibility and ease of use. Included is the **Query Builder** wizard which creates and runs queries that result in user-configured data in user-configured charts and tables.

To get you started, McAfee includes a set of default queries which provide the same information as the default reports of previous versions.

Are you setting up queries for the first time?

When setting up queries for the first time:

- Understand the functionality of queries and the **Query Builder** wizard.
- Review the default queries, and edit any to your needs.
- Create queries for any needs that aren't met by the default queries.

Contents

- ▶ [Queries](#)
- ▶ [Query Builder](#)
- ▶ [Multi-server roll-up querying](#)
- ▶ [Preparing for roll-up querying](#)
- ▶ [Working with queries](#)
- ▶ [Default queries and what they display](#)

Queries

Queries are configurable objects that retrieve and display data from the database. The results of queries are displayed in charts and tables. Any query's results can be exported to a variety of formats, any of which can be downloaded or sent as an attachment to an email message. Some queries can be used as dashboard monitors.

Query results are actionable

Query results are now actionable. Query results displayed in tables (and drill-down tables) have a variety of actions available for selected items in the table. For example, you can deploy agents to systems in a table of query results. Actions are available at the bottom of the results page.

Queries as dashboard monitors

Use almost any query (except those using a table to display the initial results) as a dashboard monitor. Dashboard monitors refresh automatically on a user-configured interval (five minutes by default).

Exported results

Query results can be exported to four different formats. Exported results are historical data and are not refreshed like when using queries as dashboard monitors. Like query results and query-based monitors displayed in the console, you can drill down into the HTML exports for more detailed information.

Unlike query results in the console, data in exported reports is not actionable.

Reports are available in several formats:

- CSV — Use this format to use the data in a spreadsheet application (for example, Microsoft Excel).
- XML — Use this format to transform the data for other purposes.
- HTML — Use this report format to view the exported results as a web page.
- PDF — Use this report format when you need to print the results.

Sharing queries between servers

Any query can be imported and exported, allowing you to share queries between servers. Any query needs to be created only once in a multi-server environment.

Public and personal queries

Queries can be personal or public. Private queries exist in the user's **My Queries** list, and are only available to their creator. Public queries exist in the **Public Queries** list, and are available to everyone who has permissions to use public queries.

Most default queries are only made available to the global administrator, who must make these default queries public for other users to access them. Several queries are public by default for use by the default dashboards.

Only users with appropriate permissions can make their personal queries public ones.

Query permissions

Use query permissions to assign specific levels of query functionality to permission sets, which are assigned to individual users.

Available permissions include:

- **No permissions** — The **Query** tab is unavailable to a user with no permissions.
- **Use public queries** — Grants permission to use any queries that have been created and made public by users with the same permissions.
- **Use public queries; create and edit personal queries** — Grants permission to use any queries that have been created and made public by users with the same permissions, as well as the ability to use the **Query Builder** wizard to create and edit personal queries.
- **Edit public queries; create and edit personal queries; make personal queries public** — Grants permission to use and edit any public queries, create and edit any personal queries, as well as the ability to make any personal query available to anyone with access to public queries.

NOTE: To run some queries, you also need permissions to the feature sets associated with their result types. Also, in a query's results pages, the available actions to take on the resulting items depend on the feature sets a user has permission to.

Query Builder

ePolicy Orchestrator provides an easy, four-step builder with which to create and edit custom queries. With the wizard you can configure which data is retrieved and displayed, and how it is displayed.

Result types

The first selection you make in the **Query Builder** wizard is a result type. This selection identifies what type of data the query will be retrieving. This selection determines what the available selections are in the rest of the wizard.

Result types include:

- Audit Log Entries — Retrieves information on changes and actions made by ePO users.
- Compliance History — Retrieves information on compliance counts over time. This query type and its results depend on a Run Query server task that generates compliance events from the results of a (Boolean pie chart) query. Additionally, when creating a Compliance History query, be sure the time unit matches the schedule interval for the server task. McAfee recommends creating the Boolean pie chart query first, followed by the server task that generates the compliance events, and finally the Compliance History query.
- Events — Retrieves information on events sent from managed systems.
- Managed Systems — Retrieves information about systems running the McAfee Security Agent.
- Notifications — Retrieves information on sent notifications.
- Repositories — Retrieves data on repositories and their status.
- Rolled-up Compliance History — Retrieves information on compliance counts over time from registered ePO servers. This query depends on server tasks being run on this ePO server and the registered servers.
- Rolled-up Managed Systems — Retrieves summary information on systems from registered ePO servers.

Chart types

ePolicy Orchestrator provides a number of charts and tables to display the data it retrieves. These and their drill-down tables are highly configurable.

NOTE: Tables do not include drill-down tables.

Chart types include:

- Bar chart
- Boolean pie chart
- Grouped bar chart
- Grouped summary table
- Line chart
- Pie chart
- Summary table
- Table

Table columns

Specify columns for the table. If you select **Table** as the primary display of the data, this configures that table. If you selected a type of chart as the primary display of data, this configures the drill-down table.

Query results displayed in a table are actionable. For example, if the table is populated with systems, you can deploy or wake up agents on those systems directly from the table.

Filters

Specify criteria by selecting properties and operators to limit the data retrieved by the query.

Multi-server roll-up querying

ePolicy Orchestrator® software version 4.0.2 now includes the ability to run queries that report on summary data from multiple ePO databases. There are these result types in the Query Builder wizard that you can use for this type of querying:

- Rolled Up Managed Systems
- Rolled Up Compliance History

Query results from these types of queries are not actionable.

How it works

To roll up data for use by roll-up queries, you must register each server (including the local server) you want to include in the querying.

Once the servers are registered, then you must configure Data Roll Up server tasks on the reporting server (the server that performs the multi-server reporting). Data Roll Up server tasks retrieve the information from all databases involved in the reporting, and populates the `eporollup_` tables on the reporting server.

The roll-up queries target these database tables on the reporting server.

NOTE: Use of the Rolled Up Compliance History type of query, requires an additional query (on Managed Systems with a Boolean pie chart) and an additional Run Query server task (with the subaction to generate a compliance event) to run on each server whose data you want to include in the Rolled Up Compliance History type of query.

Preparing for roll-up querying

Use these tasks to ensure the `eporollup_` tables on the reporting server are populated and ready for using queries based on the Rolled Up query result types. These tasks should be performed for each server whose data will be included in the query results.

NOTE: Using the Rolled-Up Compliance History result type additionally requires that a Boolean pie chart-based query on managed systems be created on each server. Additionally, on each server, a Run Query server task needs to be created with a subaction to generate compliance events based on this query.

Tasks

- [Registering ePO servers](#)

► [Creating a Data Roll Up server task](#)

Registering ePO servers

Use this task to register each ePO server with the reporting server that you want to include in roll-up queries. You must also register the reporting server. Registering the servers ensures that summary data can be taken from each to populate the `eporollup_` tables in the local database.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Network | Registered Servers**, then click **New Server**. The **Registered Server Builder** wizard appears.
- 2 Select the server type and type a name and description, then click **Next**. The **Details** page appears.
- 3 Provide the details of the server, its database server, and the credentials to access the server, then click **Save**.

Creating a Data Roll Up server task

Use this task to create a Data Roll Up server task that populates the necessary tables on the reporting server with summary data from registered servers.

Best practices

McAfee recommends creating a Roll Up Data server task on this server for each registered servers. This task would include each of the desired Roll Up Data actions, each targeting only one of the registered servers.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Automation | Server Tasks**, then click **New Task**. The **Server Task Builder** wizard appears.
- 2 Type a name and description for the task, and select whether to enable it, then click **Next**. The **Actions** page appears.
- 3 Select the desired Data Roll Up actions, and select the desired registered server to which it applies.

NOTE: McAfee recommends creating one server task per registered server, and configuring it to run both Roll Up Data actions.

- 4 Click **Next**. The **Schedule** page appears.
- 5 Schedule the task as needed, then click **Next**. The **Summary** page appears.

NOTE: If you are rolling up compliance history data, ensure that the time unit of the Roll-Up Compliance History query matches the schedule type of the Generate Compliance Event server tasks on the registered servers.

- 6 Review the settings, then click **Save**.

Working with queries

Use these tasks to create, use, and manage queries.

Tasks

- ▶ [Creating custom queries](#)
- ▶ [Running an existing query](#)
- ▶ [Running a query on a schedule](#)
- ▶ [Making personal queries public](#)
- ▶ [Duplicating queries](#)
- ▶ [Sharing a query between ePO servers](#)

Creating custom queries

Use this task to create custom queries with the Query Builder wizard. You can query on system properties, product properties, many of the log files, repositories, and more.

Task

For option definitions, click ? on the page displaying the options.

- 1** Go to **Reporting | Queries**, then click **New Query**. The **Result Type** page of the **Query Builder** wizard appears.
- 2** Select the data type for this query. This choice determines the options available on subsequent pages of the wizard.
- 3** Click **Next**. The **Chart** page appears.
- 4** Select the type of chart or table to display the primary results of the query. Depending on the type of chart, there are different configuration options available.
- 5** Click **Next**. The **Columns** page appears.
- 6** Select the properties from the **Available Columns** list that you want as columns in the results table, then order them as desired with the arrow icons on the column headers.

NOTE: If you select **Table** on the **Chart** page, the columns you select here are the columns of that table. Otherwise, these are the columns of the drill-down table.

- 7** Click **Next**. The **Filter** page appears.
- 8** Select properties to narrow the search results. Selected properties appear in the content pane with operators to specify criteria to narrow the data that is returned for that property. Ensure your choices provide the data to display in the table columns configured in the previous step.
- 9** Click **Run**. The **Unsaved Query** page displays the results of the query, which is actionable, so you can take any available actions on items in any tables or drill-down tables.
 - If this is a query you want to use again, click **Save** to add it to your **My Queries** list.
 - If the query didn't appear to return the expected results, click **Edit Query** to go back to the **Query Builder** and edit the details of this query.
 - If you don't need to save the query, click **Close**.

Running an existing query

Use this task to run an existing query from the **Queries** page.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Reporting | Queries**, then select a query from the **Queries** list.
- 2 Click **Run**. The query results appear. Drill down into the report and take actions on items as necessary. Available actions depend on the permissions of the user.
- 3 Click **Close** when finished.

Running a query on a schedule

Use this task to create and schedule a server task that runs a query and takes actions on the query results.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Automation | Server Tasks**, then click **New Task**. The **Description** page of the **Task Builder** wizard appears.
- 2 Name and describe the task, then click **Next**. The **Actions** page appears.
- 3 Select **Run Query** from the drop-down list.
- 4 Select the desired query to run.
- 5 Select the language in which to display the results.

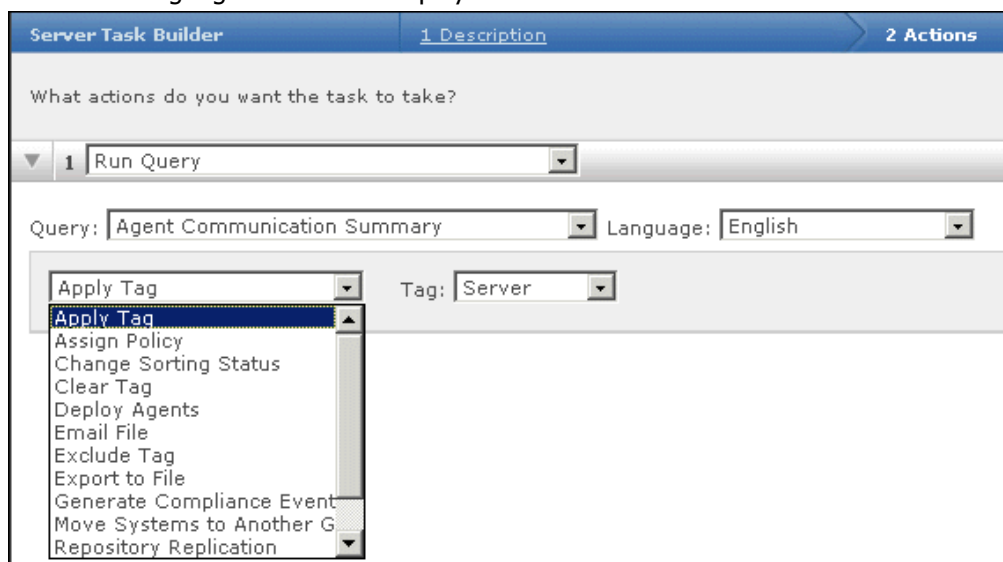


Figure 7: Run Query server task actions

- 6 Select an action to take on the results. Available actions depend on the permissions of the user, and include:
 - **Email File** — Sends the results of the query to a specified recipient, in a user-configured format (PDF, XML, CSV, or HTML).

- **Move To** — Moves all systems in the query results to a group in the System Tree. This option is only valid for queries that result in a table of systems.
- **Change Sorting Status** — Enables or disables System Tree sorting on all systems in the query results. This option is only valid for queries that result in a table of systems.
- **Exclude Tag** — Excludes a specified tag from all systems in the query results. This option is only valid for queries that result in a table of systems.
- **Generate Compliance Event** — Generates an event based on a percentage or actual number threshold of systems that do not match the criteria in the query. This action is intended for compliance-based Boolean pie chart queries that retrieve data on managed systems (for example, the ePO: Compliance Summary default query). This action is part of the replacement of the Compliance Check server task of previous versions of Policy Auditor.
- **Repository Replication** — Replicates master repository contents to the distributed repositories in the query results. This is valuable for queries that return a list of out-of-date repositories (for example, the ePO: Distributed Repository Status default query). This option is only valid for queries that result in a table of distributed repositories.
- **Clear Tag** — Removes a specified tag from all systems in the query results. This option is only valid for queries that result in a table of systems.
- **Assign Policy** — Assigns a specified policy to all systems in the query results. This option is only valid for queries that result in a table of systems.
- **Export to File** — Exports the query results to a specified format. The exported file is placed in a location specified in the Printing and Exporting server settings.
- **Apply Tag** — Applies a specified tag to all systems (that are not excluded from the tag) in the query results. This option is only valid for queries that result in a table of systems.
- **Edit Description** — Overwrites the existing system description in the database for all systems in the query results. This option is only valid for queries that result in a table of systems.
- **Deploy Agents** — Deploys agents, according to the configuration on this page, to systems in the query results. This option is only valid for queries that result in a table of systems.
- **Wake Up Agents** — Sends an agent wake-up call, according to the configuration on this page, to all systems in the query results. This option is only valid for queries that result in a table of systems.

NOTE: You are not limited to selecting one action for the query results. Click the **+** button to add additional actions to take on the query results. Be careful to ensure you place the actions in the order you want them to be taken on the query results.

- 7 Click **Next**. The **Schedule** page appears.
- 8 Schedule the task as desired, then click **Next**. The **Summary** page appears.
- 9 Verify the configuration of the task, then click **Save**.

The task is added to the list on the **Server Tasks** page. If the task is enabled (by default), it runs at the next scheduled time. If the task is disabled, it only runs by clicking **Run** next to the task on the **Server Tasks** page.

Making personal queries public

Use this task to make personal queries public. All users with permissions to public queries have access to any personal queries you make public.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Reporting | Queries**, then select the desired query from the **My Queries** list.
- 2 Click **Make Public** at the bottom of the page.

NOTE: To access the **Make Public** action, you may need to click **More Actions**.

- 3 Click **OK** in the **Action** panel when prompted.

The query is added to the **Public Queries** list. All users that have access to public queries now have access to the query.

Duplicating queries

Use this task to create a query based on an existing query.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Reporting | Queries**, then select the desired query from the **Queries** list.
- 2 Click **Duplicate**, provide a name for the duplicate, then click **OK**.
- 3 Select the new query in the **Queries** list, then click **Edit**. The **Query Builder** wizard appears with settings identical to those of the query that was the source for the duplicate.
- 4 Edit the query as desired, then click **Save**.

Sharing a query between ePO servers

Use these tasks to import and export a query for use among multiple servers.

Tasks

- ▶ [Exporting queries for use by another ePO server](#)
- ▶ [Importing queries](#)

Exporting queries for use by another ePO server

Use this task to export a query to an XML file which can be imported to another ePO server.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Reporting | Queries**, then select a query from the **Queries** list.

- 2 Click **Export**, then **OK** in the **Action** panel. The **File Download** dialog box appears.
- 3 Click **Save**, select the desired location for the XML file, then click **OK**.

The file is saved in the specified location.

Importing queries

Use this task to import a query that was exported from another ePO server.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Reporting | Queries**, then click **Import Query**. The **Import Query** dialog box appears.
- 2 Click **Browse**. The **Choose File** dialog box appears.
- 3 Select the exported file, then click **OK**.
- 4 Click **OK**.

The query is added to the **My Queries** list.

Exporting query results to other formats

Use this task to export query results for other purposes. You can export to HTML and PDF finals for viewing formats, or to CSV or XML files for using and transforming the data in other applications.

Task

For option definitions, click ? on the page displaying the options.

- 1 From the page displaying the query results, select **Export Table** or **Export Data** from the **Options** menu. The **Export** page appears.
- 2 Select whether the data files are exported individually or in a single archive (ZIP) file.
- 3 If needed, select whether to export the chart data only, or the chart data and drill-down tables.
- 4 Select the format of the exported file. If exporting to a PDF file, select the page size and orientation.
- 5 Select whether the files are emailed as attachments to selected recipients, or whether they are saved to a location on the server to which a link is provided. You can open or save the file to another location by right-clicking it.

NOTE: When typing multiple email addresses for recipients, you must separate entries with a comma or semi-colon.

- 6 Click **Export**.

The files are created and either emailed as attachments to the recipients, or you are taken to a page where you can access the files from links.

Default queries and what they display

Policy Auditor ships with a number of default queries that can be used for some of your most common needs. Each of these queries yields data that can be drilled down multiple times to show increasingly more detailed data.

PA: Benchmark Checks

Use this query to view a list of checks and the number of times they are used in a benchmark.

Query results

The results of the query are displayed in a bar chart, with each bar representing a benchmark. The height of each bar corresponds to the number of checks in the benchmark. Click a bar or a check name to view details about the benchmark.

PA: Benchmark Rules

Use this query to view the number of times a rule is included in a benchmark.

Query results

The results of the query are displayed in a bar chart, with each bar representing a benchmark. The height of each bar corresponds to the number of rules in a benchmark. Click a bar or a benchmark name to show details about the benchmark.

PA: Checks Across Benchmarks

Use this query to view the number of times a check is used in a benchmark.

Query results

This query displays a list of checks along with a count of their usage in benchmarks. The results of the query are displayed in a summary table that shows how often a query is used. Double-click a check to take you to a screen showing details about which benchmarks or profiles within a benchmark that use the check. Double-click a check to show details about the check.

PA: Check Catalog List

Use this page to view the number of checks and to view information about them.

Query results

The results of the query are displayed in a list of checks. Click a check to view information and to perform actions upon it.

Option definitions

Option	Definition
Apply Labels	Apply labels to check
Delete	Delete the check

Option	Definition
Export	Export the check in a ZIP format
Remove Labels	Remove labels from check

PA: Check Catalog Usage List

Use this page to view a list of OVAL checks and its rule and benchmark associations

Query results

The results of the query are displayed in a list of checks. Click a check to view information on it. You can perform actions upon a check.

Option definitions

Option	Definition
Apply Labels	Apply labels to check
Delete	Delete the check
Export	Export the check in a ZIP format
Remove Labels	Remove labels from check

PA: Systems by Audit

Use this query to display the systems assigned to an audit.

Query results

The results of the query are displayed in a bar chart where each bar represents an audit. Click a bar or audit name to view the systems assigned to the audit.

PA: Trend of Benchmarks Reported as Failed

Use this query, with its default settings, to view the percentage of systems (over time) in your environment that are non-compliant.

Before you begin

This query and its results depend on the Generate Compliance Event server task. Schedule this server task to run at a regular interval. This query depends on a Boolean pie chart query based on managed systems (for example, the default ePO: Compliance Summary query).

Query results

The results of the query are displayed in a line chart. Details depend on the defined compliance of the ePO: Compliance Summary query.

PA: Trend of Checks Reporting as False

Use this query, with its default settings, to view the percentage of systems (over time) in your environment that are non-compliant.

Before you begin

This query and its results depend on the Generate Compliance Event server task. Schedule this server task to run at a regular interval. This query depends on a Boolean pie chart query based on managed systems (for example, the default ePO: Compliance Summary query).

Query results

The results of the query are displayed in a line chart. Details depend on the defined compliance of the ePO: Compliance Summary query.

PA: Trend of Rules Reporting as Failed

Use this query, with its default settings, to view the percentage of systems (over time) in your environment that are non-compliant.

Before you begin

This query and its results depend on the Generate Compliance Event server task. Schedule this server task to run at a regular interval. This query depends on a Boolean pie chart query based on managed systems (for example, the default ePO: Compliance Summary query).

Query results

The results of the query are displayed in a line chart. Details depend upon the defined compliance of the ePO: Compliance Summary query.

Assessing Your Environment With Dashboards

Dashboards allow you to keep a constant eye on your environment. Dashboards are collections of monitors. Monitors can be anything from a chart-based query, to a small web application, like the MyAvert Security Threats, that is refreshed at a user-configured interval.

Users must have the appropriate permissions to use and create dashboards.

Are you setting up dashboards for the first time?

When setting up dashboards for the first time:

- Review the conceptual topics in this section to better understand dashboards and dashboard monitors.
- Decide which default dashboards and default monitors you want to use.
- Create any needed dashboards and their monitors, and be sure to make active any you want available as tabs from the navigation bar.

Contents

- ▶ [Dashboards and how they work](#)
- ▶ [Setting up dashboard access and behavior](#)
- ▶ [Working with Dashboards](#)

Dashboards and how they work

Dashboards are collections of user-selected and configured monitors that provide current data about your environment.

Queries as dashboard monitors

Use any chart-based query as a dashboard that refreshes at a user-configured frequency, so you can use your most useful queries on a live dashboard.

Default dashboard monitors

This release of ePolicy Orchestrator ships with several default monitors:

- MyAvert Security Threats — Keeps you aware of which DATs and engines are available, what threats they protect, and the versions that are currently in your master repository.
- Quick System Search — A text-based search field that allows you to search for systems by system name, IP address, MAC address, or user name.

- McAfee Links — Hyperlinks to McAfee sites, including ePolicy Orchestrator Support, Avert Labs WebImmune, and Avert Labs Threat Library.

Setting up dashboard access and behavior

Use these tasks to ensure users have the appropriate access to dashboards, and how often dashboards are refreshed.

Tasks

- ▶ [Giving users permissions to dashboards](#)
- ▶ [Configuring the refresh frequency of dashboards](#)

Giving users permissions to dashboards

Use this task to give users the needed permissions to dashboards. For a user to be able to access or use dashboards, they must have the appropriate permissions.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Configuration | Permission Sets**, then click **New Permission Set** or select a permission set in the **Permission Sets** list.
- 2 Next to **Dashboards**, click **Edit**. The **Edit Permission Set: Dashboards** page appears.
- 3 Select a permission:
 - **No permissions**
 - **Use public dashboards**
 - **Use public dashboards; create and edit personal dashboards**
 - **Edit public dashboards; create and edit personal dashboards; make personal dashboards public**
- 4 Click **Save**.

Configuring the refresh frequency of dashboards

Use this task to configure how often (in minutes) a user's dashboards are refreshed. This setting is unique to each user account.

When setting this, consider the number of users that you anticipate will be logged on at anytime. Each user logged on with a dashboard displayed creates additional performance usage when the dashboards are refreshed.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Dashboards**, then select **Edit Dashboard Preferences** from the **Options** drop-down list. The **Dashboard Preferences** page appears.
- 2 Next to **Dashboard page refresh interval**, type the number of minutes you want between refreshes.
- 3 Click **Save**.

Working with Dashboards

Use these tasks to create and manage dashboards.

Tasks

- ▶ Creating dashboards
- ▶ Making a dashboard active
- ▶ Selecting all active dashboards
- ▶ Making a dashboard public

Creating dashboards

Use this task to create a dashboard.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Dashboards**, then select **Manage Dashboards** from the **Options** drop-down list. The **Manage Dashboards** page appears.

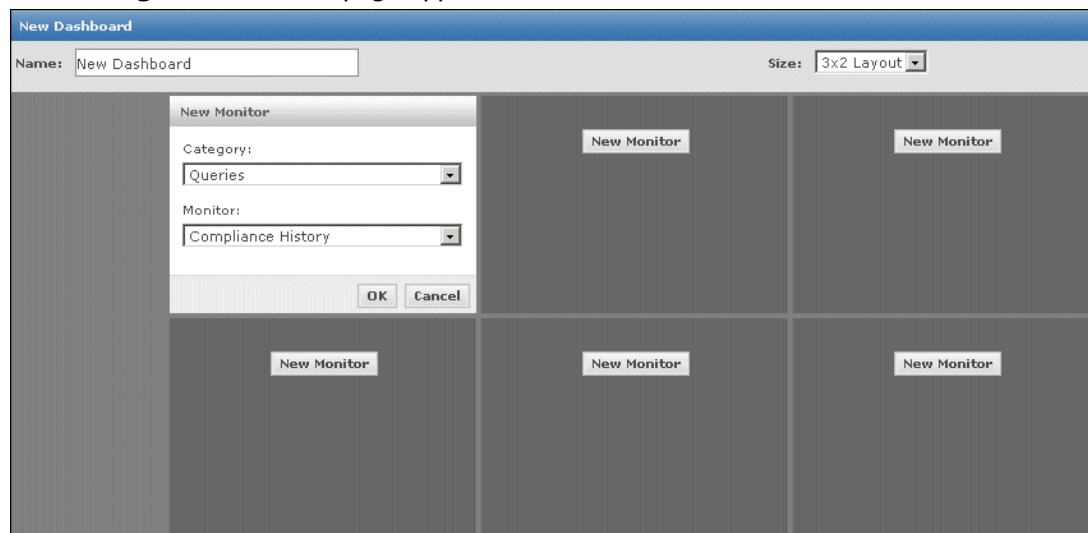


Figure 8: New Dashboard page

- 2 Click **New Dashboard**.
- 3 Type a name, and select a size for the dashboard.
- 4 For each monitor, click **New Monitor**, then select the monitor to display in the dashboard.
- 5 Click **Save**, then select whether to make this dashboard active. Active dashboards display on the tab bar of **Dashboards**.

Making a dashboard active

Use this task to make a dashboard part of your active set.

Task

For option definitions, click ? on the page displaying them.

- 1 Go to **Dashboards**, click **Options**, then select **Manage Dashboards**. The **Manage Dashboards** page appears.
- 2 Select a dashboard from the **Dashboards** list, then click **Make Active**.
- 3 Click **OK** when prompted.
- 4 Click **Close**.

The selected dashboard is now on the tab bar.

Selecting all active dashboards

Use this task to select all dashboards that make up your active set. Active dashboards are accessible from on the tab bar under **Dashboards**.

Task

For option definitions, click ? on the page displaying the options.

- 1 Go to **Dashboards**, then select **Select Active Dashboards** from the **Options** drop-down list.

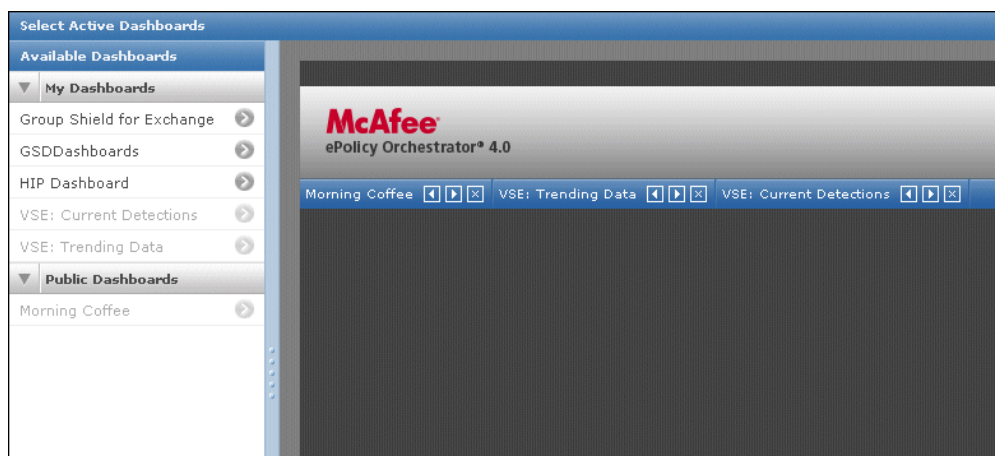


Figure 9: Select Active Dashboards page

- 2 Click the desired dashboards from the **Available Dashboards** list. They are added to the content pane.
- 3 Repeat until all desired dashboards are selected.
- 4 Arrange the selected dashboards in the order you want them to appear on the tab bar.
- 5 Click **OK**.

The selected dashboards appear on the tab bar whenever you go to the **Dashboards** section of the product.

Making a dashboard public

Use this task to make a private dashboard public. Public dashboards can be used by any user with permissions to public dashboards.

Task

For option definitions, click **?** on the page displaying the options.

- 1 Go to **Dashboards**, then select **Manage Dashboards** from the **Options** drop-down list.
- 2 Select the desired dashboard from the **Available Dashboards** list, then click **Make Public**.
- 3 Click **OK** when prompted.

The dashboard appears in the **Public Dashboards** list on the **Manage Dashboards** page.

Index

A

- absolute scoring model [44](#)
- agent plug-in
 - overview [22](#)
 - responsibilities [22](#)
- audience [10](#)
- audit
 - create [38](#)
- audit benchmarks pane
 - benchmark ID [35](#)
 - fail [35](#)
 - pass [35](#)
 - profile ID [35](#)
 - unknown [35](#)
- audit creation
 - assign benchmark profiles [34](#)
 - filter benchmarks based on labels [34](#)
- audit editing
 - assign benchmark profiles [34](#)
 - filter benchmarks based on labels [34](#)
- audit exports
 - to OVAL [36](#), [37](#)
 - to XCCDF [36](#), [37](#)
- audit label [14](#)
- Audit Log [75](#)
- audit queries
 - systems [84](#)
- audit results
 - exporting [36](#), [37](#)
- audit score [13](#)
- audit score categories [13](#)
- audits
 - absolute scoring model [44](#)
 - Audits tab [30](#)
 - benchmarks [31](#)
 - blackout times [34](#)
 - changing scoring model [44](#)
 - concept [31](#)
 - creating and managing [30](#)
 - default scoring model [43](#)
 - defining frequency [41](#)
 - editing [39](#), [40](#), [41](#)
 - exclude systems [32](#)
 - flat scoring model [43](#)
 - flat unweighted scoring model [13](#), [43](#), [44](#)
 - frequency [34](#)
 - include systems [32](#)
 - selecting benchmarks [40](#)
 - selecting systems [40](#)
 - setting whiteout and blackout [36](#)
 - whiteout times [34](#)
- Audits tab [30](#)

B

- benchmark checks,
 - queries [83](#)
- Benchmark Editor
 - about [9](#)
 - activating benchmarks [9](#)
 - editing benchmarks [9](#)
 - Policy Auditor, component [9](#)
 - tailoring benchmarks [9](#)
- benchmark rules,
 - queries [83](#)
- benchmarks
 - about [9](#)
 - activating [9](#)
 - concept [12](#), [42](#)
 - editing [9](#)
 - not required for exemption waivers [47](#)
 - required for exception waivers [47](#)
 - required for suppression waivers [48](#)
 - selecting for a new audit [38](#)
 - tailoring [9](#)
 - used in audits [31](#)
 - waivers [46](#), [48](#), [51](#)
- blackout
 - concept [34](#)
- blackout period
 - setting [36](#)

C

- CCE Implementation [20](#)
- changing scoring model [44](#)
- charts (See queries) [75](#)
- checks
 - use in audits [31](#)
- checks, queries [83](#)
- compliance
 - history, queries [84](#), [85](#)
- components
 - Benchmark Editor [9](#)
 - Benchmark Editor, about [9](#)
 - Policy Auditor [9](#)
 - Policy Auditor Agent plug-in [9](#)
- content for Policy Auditor [23](#)
- CPE Implementation [20](#)
- creating
 - Policy Auditor Plug-in deployment task [25](#), [27](#)
- creating a new audit
 - defining frequency [39](#)
 - saving [39](#)
 - selecting benchmarks [38](#)
 - selecting systems [38](#)
- creating audits
 - assign benchmark profiles [34](#)
- creating waivers [51](#)

CVE Implementation [20](#)
 CVSS Implementation [20](#)

D

dashboards
 active set [89](#)
 chart-based queries and [86](#)
 configuring access and behavior [87](#)
 configuring refresh frequency [87](#)
 creating [88](#)
 default monitors [86](#)
 granting permissions to [87](#)
 how they work [86](#)
 making active [88](#)
 making public [89](#)
 selecting all in a set [89](#)
 data retention [14](#)
 Data Roll-Up server task [77](#)
 databases
 multi-server querying [76](#)
 public and personal queries [74](#)
 queries and retrieving data [73](#)
 registering servers for roll-up queries [77](#)
 default scoring model [43](#)
 defining frequency for audits [39, 41](#)
 deleting waivers [53](#)

E

editing an audit
 assign benchmark profiles [34](#)
 name and describe [39, 41](#)
 saving [41](#)
 editing audits [39, 40, 41](#)
 editing server settings [16](#)
 exception waivers [47, 48](#)
 benchmark and rule [47](#)
 effect on audit results [47](#)
 effect on scoring [47](#)
 expires date [48](#)
 start date [48](#)
 exemption waivers [47](#)
 effect on audit results [47](#)
 effect on scoring [47](#)
 expired status for waivers [46](#)
 expires date for waivers [46, 49, 51](#)
 expiring waivers [53](#)
 exporting audit results [36, 37](#)

F

FDCC Implementation [19](#)
 filtering waivers [49, 50, 51](#)
 by date [50](#)
 by group [51](#)
 by status [50](#)
 filters
 query results [76](#)
 flat scoring model [43](#)
 flat unweighted scoring model [13, 43, 44](#)
 frequency
 concept [34](#)

G

granting waivers [52](#)

I

in-effect status for waivers [46](#)
 include systems in audits
 add group [32](#)
 add system [32](#)
 add tag [32](#)
 specify criteria [32](#)
 IP address
 waivers [51](#)
 issues
 about [54](#)
 adding comments to [62](#)
 adding tickets to [71](#)
 assigning [62](#)
 associations with tickets (See ticketed issues) [55](#)
 creating [60](#)
 creating automatically with responses [61](#)
 deleting [63](#)
 details of, viewing [62](#)
 editing [63](#)
 how they are created [54](#)
 how they are managed [55](#)
 purging closed [63](#)
 purging closed on a schedule [63](#)
 ticketing servers (See ticketing servers) [54](#)
 Issues tab
 granting waivers [52](#)

M

MAC address
 waivers [51](#)
 Make Public action [81](#)
 managed system
 deleting waivers [53](#)
 expiring waivers [53](#)
 filtering waivers [49, 50, 51](#)
 waivers [46, 51, 52](#)
 managed systems
 roll-up querying [76](#)
 McAfee Links, default monitor [86](#)
 McAfee recommendations
 create a Roll Up Data server task [77](#)
 monitors (See dashboards) [86](#)
 MyAvert Threat Service, default monitor [86](#)

N

name and describe an audit [39, 41](#)

O

OVAL
 exporting audit results [36, 37](#)
 use in audits [31](#)
 OVAL Implementation [21](#)

P

permission set
 built-in for Policy Auditor [15](#)
 create [14, 16](#)
 delete [18](#)
 duplicate [17](#)
 edit [17](#)
 permissions
 for queries [74](#)

- permissions (*continued*)
 - to dashboards [87](#)
- policy auditor
 - agent plug-in responsibilities [22](#)
- Policy Auditor
 - agent plug-in [9](#)
 - agent plug-in overview [22](#)
 - audience [10](#)
 - concept [9](#)
 - managing content [23](#)
 - product guide, using [10](#)
 - supported platforms [23](#)
- Policy Auditor Agent plug-in
 - Policy Auditor, component [9](#)
- Policy Auditor Agent Plug-in
 - about [9](#)
 - overview [22](#)
- Policy Auditor Plug-in
 - agent-server communication [26](#)
 - deploying [25](#)
 - deployment, checking progress [26](#)
 - deployment, verifying [26](#)
 - installation, agent-server communication [26](#)
 - installation, checking progress [26](#)
 - installation, verifying [26](#)
 - installing [25](#)
 - remove, checking progress [28](#)
 - remove, verifying [28](#)
 - removing [27](#)
 - uninstall, checking progress [28](#)
 - uninstall, verifying [28](#)
 - uninstalling [27](#)
- Policy Auditor supported platforms [23](#)

Q

- queries
 - about [73](#)
 - actions on results [73](#)
 - chart types [75](#)
 - custom, creating [78](#)
 - defaults [83](#)
 - duplicating [81](#)
 - exported as reports [74](#)
 - exporting to XML file [81](#)
 - filters [76](#)
 - importing from a server [82](#)
 - making personal queries public [81](#)
 - My Queries list [74](#)
 - permissions [74](#)
 - preparing for roll-up queries [76](#)
 - public and personal [74](#)
 - Public Querieslist [74](#)
 - registering ePO servers [77](#)
 - report formats [74](#)
 - results as dashboard monitors [73](#)
 - results as tables [76](#)
 - roll-up from multiple servers [76](#)
 - running existing [79](#)
 - scheduled [79](#)
- Query Builder wizard
 - about [75](#)
 - creating custom queries [78](#)
 - resulttypes [75](#)
- query names
 - Compliance History [84](#)

- query names (*continued*)
 - Trend of Benchmarks Reported as Failed [84](#)
- querynames
 - Benchmark Rules [83](#)
 - Checks Across Benchmarks [83](#)
 - Compliance History [85](#)
 - Systems by Audit [84](#)
- Quick System Search dialog [51](#)
- Quick System Search, default monitor [86](#)

R

- Remedy
 - sample mapping for (See ticketing servers) [58](#)
- reports
 - exportedquery results [74](#)
 - formats [74](#)
- requested status for waivers [46](#)
- requesting waivers [51](#)
- Results Timeframe control [35](#)
- roll-up queries (See queries) [76](#)
- rule
 - example [31](#)
- rules
 - about [9](#)
 - not required for exemption waivers [47](#)
 - required for exception waivers [47](#)
 - required for suppression waivers [48](#)
 - use in audits [31](#)
 - waivers [46](#), [48](#), [51](#)

S

- saving a new audit [39](#)
- saving an audit [41](#)
- SCAP Compliance
 - CCE [20](#)
 - CPE [20](#)
 - CVE [20](#)
 - CVSS [20](#)
 - FDCC [19](#)
 - OVAL [21](#)
 - overview [19](#)
 - XCCDF [21](#)
- SCAP Implementation [19](#)
- score computation [13](#), [43](#)
- scoring
 - absolute scoring model [44](#)
 - changing scoring model [44](#)
 - default scoring model [43](#)
 - flat scoring model [43](#)
 - flat unweighted scoring model [13](#), [43](#), [44](#)
- selecting benchmarks for a new audits [38](#)
- selecting benchmarks for audits [40](#)
- selecting systems for audits [40](#)
- selecting systems for new benchmarks [38](#)
- server setting
 - audit label [14](#)
 - audit score [13](#)
 - audit score categories [13](#)
 - categories [13](#)
 - data retention [14](#)
 - default scoring model [13](#)
 - stop data maintenance [14](#)
- server settings
 - editing [16](#)

- server tasks
 - scheduling a query [79](#)
- servers
 - importing and exporting queries [81](#)
 - registering, for queries [77](#)
 - roll-up queries [77](#)
- servertasks
 - Data Roll-Up [77](#)
- Service Desk
 - sample mappings for (See ticketing servers) [59](#)
- start date for waivers [46](#), [49](#), [51](#)
- status
 - expired [53](#)
 - in-effect [53](#)
 - requested [48](#)
 - upcoming [53](#)
 - waivers [51](#), [52](#)
- status, waivers
 - expired [46](#)
 - in-effect [46](#)
 - requested [46](#)
 - upcoming [46](#)
- stop data maintenance [14](#)
- SuperAgents
 - wake-up calls to System Tree groups [24](#)
- supported platforms
 - platforms [23](#)
- suppression waivers [48](#)
 - benchmark and rule [48](#)
 - effect on audit results [48](#)
 - effect on scoring [48](#)
- system
 - deleting waivers [53](#)
 - expiring waivers [53](#)
 - waivers [46](#), [51](#), [52](#)
- system name
 - waivers [51](#)
- System Tree
 - groups and manual wake-up calls [24](#)
- systems
 - exclude from audit [32](#)
 - include in audits [32](#)

T

- ticketed issues
 - about [55](#)
 - about editing manually [56](#)
 - how comments are handled with [56](#)
 - how they are assigned [55](#)
 - how they are closed [55](#)
 - how they are created [55](#)
 - how they are reopened [56](#)
 - how they are synchronized [56](#)
 - synchronizing [72](#)
 - synchronizing on a schedule [72](#)
- ticketing servers
 - about integrations with [57](#)
 - about sample mappings [58](#)
 - configuring DNS for Service Desk 4.5 [67](#)
 - considerations when deleting [57](#)
 - installing extensions for [64](#), [67](#)
 - installing extensions for Remedy [65](#)
 - installing extensions for Service Desk [66](#)
 - mapping [67](#), [68](#)
 - mapping issues to tickets [69](#)

- ticketing servers (*continued*)
 - mapping tickets back to issue status [70](#)
 - registering [67](#), [68](#)
 - required fields for mapping [57](#)
 - sample mapping for Remedy [58](#)
 - sample mappings for Service Desk [59](#)
 - upgrading [70](#)
- tickets
 - about [55](#)
 - adding to issues [71](#)
 - associations with issues (See ticketed issues) [55](#)
 - how comments are handled with [56](#)
 - how they are closed [55](#)
 - how they are created [55](#)
 - how they are reopened [56](#)
 - how they are synchronized [56](#)
 - server integrations for (See ticketing servers) [57](#)
 - synchronizing [72](#)
 - synchronizing on a schedule [72](#)
- types of waivers [46](#), [47](#), [49](#), [51](#)
 - exception [46](#), [47](#), [49](#)
 - exemption [46](#), [47](#), [49](#)
 - suppression [46](#), [47](#), [49](#)

U

- upcoming status for waivers [46](#)
- user name
 - waivers [51](#)

V

- view rule result columns
 - systems other [35](#)
- view rule results column
 - group path [35](#)
 - rule ID [35](#)
 - systems failed [35](#)
 - systems passed [35](#)
- view system results column
 - audit date [35](#)
 - expiration date [35](#)
 - rules failed [35](#)
 - rules other [35](#)
 - rules passed [35](#)
 - score [35](#)
 - system group [35](#)
 - system name [35](#)
 - system tags [35](#)

W

- waivers
 - actions [46](#)
 - benchmark [46](#), [48](#), [51](#)
 - catalog [46](#)
 - concept [46](#), [51](#)
 - creating [51](#)
 - deleted [48](#)
 - deleting [53](#)
 - exception [46](#), [48](#)
 - exception, benchmark and rule [47](#)
 - exception, concept [47](#)
 - exception, effect on audit results [47](#)
 - exception, effect on scoring [47](#)
 - exemption [46](#), [48](#)
 - exemption, concept [47](#)

waivers (*continued*)

- exemption, effect on audit results [47](#)
- exemption, effect on scoring [47](#)
- expired [48](#), [50](#), [53](#)
- expires [46](#), [51](#)
- expires date [48](#)
- expires date, concept [49](#)
- expiring waivers [53](#)
- filtering [49](#), [50](#), [51](#)
- granted by [46](#), [51](#), [52](#)
- granting [52](#)
- in-effect [48](#), [50](#)
- name [46](#), [51](#)
- notes [46](#), [51](#)
- Quick System Search dialog [51](#)
- requested [48](#), [51](#), [52](#)
- requesting [51](#)
- rule [46](#), [48](#), [51](#)
- score computation [43](#)
- start date [46](#), [48](#), [51](#), [53](#)
- start date, concept [49](#)
- status [46](#), [51](#), [53](#)
- status, expired [48](#), [50](#)
- status, in-effect [48](#), [50](#), [52](#)

waivers (*continued*)

- status, requested [48](#), [51](#)
- status, upcoming [48](#), [50](#)
- suppression [46](#), [48](#)
- suppression, benchmark and rule [48](#)
- suppression, effect on audit results [48](#)
- suppression, effect on scoring [48](#)
- system [46](#), [51](#)
- type [46](#), [51](#)
- types [47](#), [49](#)
- upcoming [48](#), [50](#)
- waivers catalog [46](#), [48](#), [49](#), [50](#), [51](#), [52](#), [53](#)
- waivers tab [46](#), [47](#), [48](#), [49](#), [50](#), [51](#), [52](#), [53](#)
- wake-up calls
 - to System Tree groups [24](#)
- whiteout
 - concept [34](#)
- whiteout period
 - setting [36](#)

X

- XCCDF
 - exporting audit results [36](#), [37](#)
- XCCDF Implementation [21](#)

